Departamento de Informática

TRABAJO DE FIN DE GRADO

GESTIÓN DE LA CO-PROPIEDAD Y ACCESO ANÓNIMO EN FACEBOOK

Autor: Álvaro Galán Serrano

Tutora: Lorena González Manzano

Co-tutora: Almudena Alcaide Raya

Leganés, septiembre de 2013

Título: Gestión de las políticas de co-propiedad en Facebook

Autor: Álvaro Galán Serrano
Tutora: Lorena González Manzano
Co-tutora: Almudena Alaide Raya

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día __ de _____ de 20__ en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

Agradecimientos

Querría que esta sección tuviese un mayor peso en la memoria, ya que sin la ayuda de las personas que citaré a continuación, el desarrollo del trabajo de fin de grado no hubiera sido posible para mí.

A mis padres y mi hermano, por su apoyo, su ánimo y su perseverancia a lo largo de toda la carrera y también por compartir conmigo los mejores y también los peores momentos. A Blanca, por mantenerse a mi lado, por su apoyo incondicional, por sacarme de la rutina, por aguantarme en mis peores días y por conseguir animarme cuando los tenía. A todos mis amigos, por su ánimo y su calor.

También quiero agradecer a Lorena su paciencia y dedicación a este TFG, ya que ha estado disponible siempre para cualquier cuestión, me ha ayudado muchísimo y ha sido mi principal referencia. También me gustaría agradecer a Almudena y a Esther su esfuerzo por ayudarme a sacar adelante el sistema, aunque haya costado varias reuniones de más.

Por último, a todos y cada uno de mis compañeros de clase, por los cuatro años que he vivido con ellos, su ayuda sincera y porque sin ellos no hubiera llegado hasta aquí. Jamás dejaré de aprender de ellos.

Resumen

Durante los últimos años, las relaciones humanas han evolucionado para producirse a través de Internet. En particular, las redes sociales facilitan su establecimiento y la compartición de contenidos multimedia. Actualmente, a la sociedad le preocupa la privacidad de los contenidos que poseen en estas redes, pero aún queda mucho por hacer; por ejemplo, ninguna red social permite gestionar la co-propiedad de los contenidos. Los usuarios involucrados en los contenidos que no les pertenecen se consideran co-propietarios.

Por otra parte, las redes sociales rastrean las acciones de los usuarios, por tanto, el anonimato es una característica inalcanzable. Una vez que los datos confidenciales de los usuarios son revelados, no volverán a ser confidenciales nunca más. Este problema actualmente no está siendo contemplado por las redes sociales, lo que agrava el problema aún más.

Por tanto, las redes sociales actuales presentan dos inconvenientes a tener en cuenta: no existe una gestión de la co-propiedad y no existe acceso anónimo.

Para abordar dos inconvenientes descritos, este trabajo de fin de grado presenta un sistema, desarrollado como aplicación de Facebook, que permite a los propietarios y lo co-propietarios gestionar conjuntamente sus contenidos compartidos y permitir el acceso anónimo a estos contenidos. La gestión de la co-propiedad está realizada mediante un sistema de votación que impide revelar las preferencias del propietario y los co-propietarios. Por otra parte, se aplica la tecnología de credenciales anónimas para permitir o denegar de forma anónima el acceso al contenido solicitado, en relación a un conjunto de características de los usuarios (los cuales poseen una credencial).

Palabras clave: anonimato, co-propiedad, políticas de control de acceso, redes sociales.

Abstract

Over the last years human relationships have evolved and Internet has become the main source of communication. In particular, Online Social Networks (OSN) facilitates the establishment of relationships and the sharing of multimedia content. Nowadays, society is concerned about their content's privacy but much more need to be done; for instance, none of a single OSN provides co-ownership management. Note that users involved in content which do not belong to them are considered co-owners.

On the other hand, OSN track users' actions and then, anonymity is an unachievable feature. Once user's confidential data are disclosed, they never become confidential anymore. This issue is not currently considered in OSN, which exacerbates the problem further.

Therefore, today's OSN have a pair of drawbacks to consider: there is no co-ownership management and there is no anonymous access.

To address above problems this final degree work presents a system, developed as a Facebook application, to allow owners and co-owners to jointly manage their shared content and to allow anonymous access to these content. Co-ownership management is performed applying a voting scheme which prevents from disclosing preferences of the owner and of the co-owners. On the other hand, anonymous credentials are applied to anonymously grant or deny access to the requested data regarding a set of users' characteristics (within a credential).

Keywords: access control policies, anonymity, co-ownership, online social networks.

Índice general

Índice de figuras

Índice de tablas

Capítulo 1

Introducción y objetivos

1.1 Introducción

Las relaciones sociales entre los seres humanos siempre han tenido una importancia especial. Desde la llegada de Internet se ha pretendido mejorar los medios para mantener la comunicación entre las personas. Este motivo dio lugar a la aparición servicios como el correo electrónico, los chats, la mensajería instantánea o los *newsgroups*. Si bien estos servicios cubrían las necesidades básicas de comunicación, se alejaban bastante de ser un medio de comunicación natural para las personas, ya que todos ellos presentaban características como el anonimato, la ausencia de señales no verbales, el distanciamiento físico y la disponibilidad del tiempo de un modo asíncrono. Aunque algunos de esos problemas son difíciles de solventar, las redes sociales han supuesto un paso hacia delante.

Durante los últimos años, las redes sociales se han convertido en un nuevo medio de comunicación, en el que se establecen múltiples relaciones sociales. Se diferencian de sus predecesores tecnológicos en que éstas permiten a sus usuarios compartir todo tipo de contenidos. Como en la vida real, en las redes sociales existen diferentes tipos de relaciones entre los usuarios, que tomarán un nombre u otro dependiendo de la red social, pero el concepto entre todas ellas es similar. Los usuarios pueden establecer relaciones, compartiendo fotografías, videos música o cualquier contenido de la red. Además, otra de las características que puede identificarse en las redes sociales es que los contenidos pueden involucrar a múltiples usuarios además del propietario. Tales usuarios son denominados "co-propietarios".

Actualmente, una de las redes sociales con mayor trascendencia es Facebook [1], siendo éste el motivo por el que el presente trabajo de fin de grado hace uso de esta red social. Su aparición en el año 2004 como una red social para los estudiantes de la Universidad de Harvard revolucionó las existentes y acabó convirtiéndose en una red abierta a todo el mundo. Las relaciones entre los usuarios de Facebook se llaman relaciones de amistad, así un usuario que está en la lista de amigos de otro, se dice que es amigo de este otro. Facebook ofrece un chat en tiempo real, un “muro” [2] y una sección de fotos, donde es posible agrupar éstas por álbumes [3]. Aprovechando las ventajas sociales que ofrece Facebook, los desarrolladores pueden crear aplicaciones e incluirlas dentro de esta red social. Existen muchas otras redes sociales, pero la importancia y la multitud de características que posee Facebook la convierte en una red social de referencia.

Si bien es cierto que esta red social ofrece una amplia gama de servicios, existe un gran problema relacionado con la privacidad de los contenidos que cada usuario posee en la red. A pesar de que existen medidas para administrar la privacidad de éstos, siguen existiendo carencias que no ofrecen una experiencia satisfactoria para los usuarios. Particularmente, en contenidos como las fotos es fácil verificar este problema. Éstas son gestionadas por su propietario, dejando a los co-propietarios al margen de dicha gestión. Este problema no sólo se identifica en Facebook, sino también en otras redes sociales tal y como se analizará en el Capítulo 2 del presente documento. Es por este motivo por el

que existen varias ramas de investigación dedicadas a la gestión de la privacidad de los contenidos tanto para los propietarios de los mismos como para los co-propietarios.

Cuando un usuario trata de acceder a un contenido, se debe comprobar si posee los privilegios adecuados para poder visualizarlo. Al conjunto de privilegios que debe poseer el usuario para poder acceder al contenido se le denomina "política de control de acceso". En la mayoría de los casos el privilegio del acceso viene dado en función de las relaciones de amistad entre el propietario del contenido y el usuario que trata de acceder. Sería interesante avanzar un paso más en lo que a políticas de control de acceso respecta, planteando comprobar atributos reales del usuario para acceder a los contenidos. Si bien esto podría resultar útil, plantea un problema mayor, ya que al revelar datos reales a la red social se cometería una violación de la privacidad del usuario. La *Ley Orgánica 15/1999* [4] dicta que se ha de proteger los datos de carácter personal de las personas físicas; por ello, lo deseable sería utilizar estos atributos para comprobar las políticas de control de acceso pero manteniendo su anonimato.

Debido a lo expuesto, se hace interesante contemplar la tecnología de credenciales anónimas. Una credencial anónima [5] es un fichero digital que almacena información real de una persona con una firma criptográfica, realizada por una autoridad, que verifica que realmente pertenece a esa persona. Esta información está basada en atributos que pueden ser públicos o privados, siendo este último tipo de atributo confidencial. Que sea confidencial significa que esta información no puede revelarse al sistema que esté verificando los datos de la credencial, y que por lo tanto deben ser tratados de forma especial para su comprobación. Es por esto por lo que se considera un gran avance desarrollar un sistema basado en credenciales anónimas para el acceso a contenidos de las redes sociales.

Este trabajo de fin de grado se centra en los álbumes de fotos porque, como ya se ha comentado anteriormente, es uno de los contenidos más sensibles que poseen los usuarios y, lamentablemente, existen grandes problemas asociados a ellos.

1.2 Motivación

El gran uso de las redes sociales plantea un gran problema para la privacidad de las personas, debido a que pueden revelarse datos de carácter personal a terceros no deseados. Con los años, los desarrolladores de las redes sociales se han preocupado por aumentar la privacidad de los datos de sus usuarios y de proporcionar mecanismos para escoger el tipo de privacidad que desean para sus contenidos.

Si bien es cierto que estos mecanismos han ayudado a los propietarios de los contenidos a escoger su privacidad, supone un problema para los co-propietarios de los de los mismos. No se dispone de ningún mecanismo que permita gestionar la privacidad de forma conjunta, tanto a propietarios como a co-propietarios. Para entender bien la importancia de un mecanismo de elección de políticas de control de acceso, se plantea el siguiente escenario ficticio: supongamos que Alicia es la propietaria de un álbum de fotos de una escapada que una gran asociación de personas con discapacidad ha realizado. Alicia, al ser la propietaria, es la única persona que puede imponer la política de control de acceso ya que es lo que permite la red social. Los co-propietarios, que son todas las personas que aparecen en el álbum, están molestos con la elección que ha realizado Alicia, ya que ha escogido una política que permite a cualquier usuario de la red social acceder a visualizar el álbum. Como es deseable, los co-propietarios desean ponerse de acuerdo para poder escoger las políticas de control de acceso, pero el sistema no se lo permite. Además, aún si el sistema lo permitiera, ninguno de ellos desearía que los demás pudieran averiguar la preferencia que cada uno ha elegido.

Teniendo en cuenta el escenario anterior, se plantea realizar un sistema que permita al propietario y los co-propietarios de un álbum de fotos de Facebook escoger una política de control de acceso de forma conjunta y que mantenga en todo momento el anonimato de los participantes. El contexto se centra en álbumes muy grandes, con información sensible y con muchos co-propietarios. Los atributos a decidir de la política serán los que siguen. La edad, donde se escogerá entre permitir el acceso a todo el mundo sin importar su edad o permitírselo a los mayores de 18 años. El grado de discapacidad, ya sea física o mental, donde se escogerá entre permitir el acceso a todas las personas, tengan o no tengan discapacidad, o permitir el acceso a aquellas que sí la tienen, es decir, que superan el 33% de discapacidad. El último atributo es la nacionalidad, donde se decide entre permitir el acceso a aquellas personas que pertenezcan a la Unión Europea o permitírselo a aquellas que no pertenezcan. La decisión de la política final estará determinada por una votación previa que deberán realizar todos. Una vez realizado este sistema quedarán solventados los problemas anteriormente mencionados. Con el fin de preservar el anonimato de los votos de cada uno, la votación se hará de forma que será imposible determinar qué ha votado cada uno de ellos.

Ahora se plantea visualizar el escenario desde el punto de vista del usuario que trata de acceder a visualizar el álbum que Alicia ha compartido, identificándose así el segundo de los problemas abordados por este trabajo. Como se ha decidido anteriormente, la política de control de acceso estará determinada en base a la edad, al grado de discapacidad y a la nacionalidad. Benito, un usuario que desea visualizar el álbum de

Alicia, trata de acceder a él usando este sistema. A pesar de que está interesado en contemplar el álbum, desconfía de hacerlo cuando es preguntado por estos atributos. Desafortunadamente, el sistema no cumple con la *Ley Orgánica 15/1999* [4], lo que no asegura que los datos serán tratados con la confidencialidad que requieren. Por este motivo Benito decide no utilizarlo ya que si muestra estos atributos a la red, dejarán de ser privados para siempre. Para que los usuarios puedan utilizar el sistema con total confianza en él, se requiere avanzar un paso más.

Es por este motivo por el que se decide desarrollar un control de acceso a los álbumes, complementario con el sistema de votación propuesto, basado en credenciales anónimas donde los datos de los usuarios que traten de acceder sean tratados de forma confidencial y no sea necesario revelarlos directamente al sistema, preservando así el anonimato de éstos.

En definitiva, se desarrollará un sistema que aportará un avance importante en la gestión de la co-propiedad y el anonimato de las redes sociales, lo que contribuirá positivamente en la sociedad actual. Además, será de mucha utilidad para la comunidad investigadora ya que no existen ramas de investigación dedicadas a fusionar el concepto del anonimato con el de co-propiedad.

1.3 Objetivos

Tras introducir el sistema que se va a desarrollar, se plantean dos grandes objetivos a satisfacer.

El primer objetivo se basa en crear un sistema de votación conjunta que permita a propietarios y co-propietarios gestionar el acceso a sus contenidos. Además, el sistema ha de integrarse en Facebook, por ser la red social con mayor relevancia actualmente. Asimismo, la elección de las preferencias de privacidad (políticas de control de acceso) ha de ser anónima, de forma que no sea posible averiguar qué ha votado cada participante. Por lo tanto este objetivo cubre lo relativo a la elección de la política de control de acceso por parte de los co-propietarios.

El segundo objetivo consiste en realizar un mecanismo de control de acceso a los álbumes del sistema basado en la comprobación de una credencial. De este modo los usuarios podrán acceder a los contenidos sin ser identificados.

1.4 Organización del presente documento

Para facilitar la lectura del presente documento, en esta sección se detalla la estructura que seguirá, organizada por capítulos y la temática de cada uno de ellos.

Capítulo 1, Introducción y objetivos: En este capítulo se realiza una introducción a las redes sociales y a los problemas de privacidad que presentan, junto con la motivación de este trabajo y los objetivos perseguidos.

Capítulo 2, Estado del arte: En este capítulo se expone el estudio realizado sobre las tecnologías utilizadas hoy día para la gestión de la co-propiedad en las redes sociales así como el estudio realizado sobre las líneas de investigación que tratan de proponer soluciones a los problemas existentes.

Capítulo 3, Análisis: En este capítulo se detalla el análisis del problema así como una perspectiva general del sistema que se deberá realizar. Se incluyen en él los componentes que deberá contener el sistema, el estudio y la elección de las tecnologías que se aplicarán, la especificación de los casos de uso, el catálogo de requisitos y las pruebas de aceptación que se deberán realizar para comprobar la correcta aplicación de los requisitos.

Capítulo 4, Diseño detallado: En este capítulo se realiza un diseño detallado de cómo va a ser el sistema final. Se incluyen los diagramas de clases de cada componente de la arquitectura y se muestran los diagramas de secuencia asociados a los casos de uso analizados.

Capítulo 5, Implementación y pruebas: En este capítulo se presentan los aspectos más importantes de la implementación del sistema así como los resultados obtenidos en las pruebas de aceptación.

Capítulo 6, Conclusiones y líneas futuras: En este capítulo se muestran las conclusiones extraídas tras la realización del trabajo de fin de grado, así como las dificultades encontradas y las posibles líneas futuras de trabajo.

Anexo 1, Gestión del proyecto: En este anexo se detalla la planificación del trabajo de fin de grado junto con el seguimiento del mismo. De forma adicional, se muestra el presupuesto del proyecto así como con las desviaciones detectadas en el mismo.

Anexo 2, Manual de usuario: En este anexo se detalla el funcionamiento del sistema paso por paso como referencia de uso para los usuarios.

Anexo 3, Plantillas: En este anexo se encuentran las plantillas utilizadas para el trabajo de fin de grado.

Capítulo 2

Estado del arte

2.1 Evaluación de la privacidad en las redes sociales actuales

Se realizará a continuación un análisis de las redes sociales más relevantes ordenadas de menor a mayor relevancia [1]. En él se analizará la gestión de las políticas de privacidad sobre las fotos individuales y sobre los álbumes, en el caso de disponer de un servicio de álbumes de fotos.

2.1.1 Bebo

Bebo (acrónimo de "Blog Early, Blog Often") es la segunda red social más importante en el Reino Unido. Ofrece un servicio de creación de perfiles y subida de contenidos muy similar al de otras redes sociales, como Facebook.

Atendiendo a las opciones de privacidad que ofrece la plataforma, se puede escoger entre que el perfil creado sea visible por todos o que únicamente lo puedan ver los amigos. Adicionalmente, se puede definir un rango de edades de contactos que pueden contactar con el usuario [6].

De esta forma, si se selecciona la opción de "Todos", todo el contenido subido a la red social será visible por cualquier usuario de ella.

Atendiendo a las fotos, se pueden subir de forma individual o en forma de álbum. Al crear el álbum de fotos se ofrecen dos opciones, no excluyentes, de privacidad: restringir el acceso al álbum para únicamente los amigos y permitir que los demás usuarios puedan copiar las fotos del álbum a sus álbumes propios.

A continuación se definirán dos escenarios para la realización de pruebas sobre la privacidad y la co-propiedad de los álbumes en esta red social.

2.1.1.1 Escenario 1

Se han creado tres perfiles falsos para realizar la prueba. El primero, "Alvaro Galan", es poseedor de un álbum en el cual están etiquetados él y su amigo, "Ags Ags". La privacidad general de "Alvaro Galan" está configurada para que su perfil sea visible por sólo sus amigos, y la privacidad general de "Ags Ags" está configurada para que su perfil sea público. La privacidad del álbum "Alvaro Galan" está configurada para que únicamente sus amigos puedan ver el álbum. La Figura 1 muestra este escenario de forma gráfica.

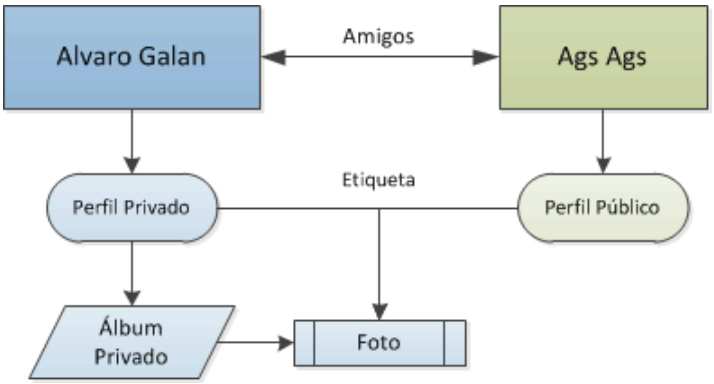

Figura 1. Escenario 1 Bebo

Ahora aparece un nuevo usuario, "Juan", que no es amigo de ninguno de los dos, pero que accede al perfil de "Ags Ags" ya que es público. Al acceder puede observar cómo "Ags Ags" ha sido etiquetado en un álbum y puede ver una vista en miniatura de la foto (Figura 2). Seguidamente "Juan" procede a visualizar la imagen pero, como el álbum es propiedad de "Alvaro Galan", el sistema le muestra un mensaje de que debe agregar a "Alvaro Galan" como amigo para visualizar el contenido, asegurando así la política restrictiva de privacidad que impuso "Alvaro Galan". "Ags Ags" no dispone de herramientas de gestión de la co-propiedad para este álbum, por lo tanto, la política más restrictiva es la que se impone.

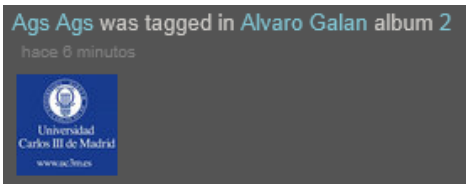

Figura 2. Perfil 1 Bebo

2.1.1.2 Escenario 2

Para continuar testeando la privacidad, se propone ahora otro escenario donde la situación cambia ligeramente con respecto al escenario número 1. En este caso es "Ags Ags" quien posee un álbum de fotos público, donde está etiquetado "Alvaro Galan". (Figura 3)

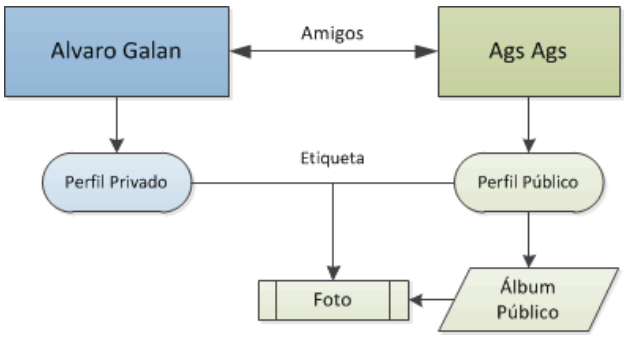

Figura 3. Escenario 2 Bebo

De igual manera que anteriormente, "Juan" trata de acceder al perfil de "Ags Ags" para visualizar el contenido, pudiendo ver de igual manera que antes la miniatura de la fotografía y la información de que ha sido etiquetado (Figura 4).

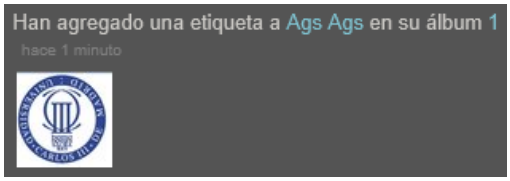

Figura 4. Perfil 2 Bebo

En este caso, "Juan" sí es capaz de visualizar la imagen y las etiquetas de ella. "Alvaro Galan" no dispone de herramientas de gestión de la co-propiedad, por lo tanto, lo único que el sistema le permite hacer es retirar su etiqueta, pero nunca gestionar la privacidad de la imagen.

Figura 5. Imagen 1 Bebo

El problema no acaba aquí, ya que si se observa con atención la Figura 5, se puede ver un hipervínculo que permite a "Juan" copiar esta imagen a uno de sus álbumes, ya que la opción de permitir que otros copien las fotos del álbum fue marcada en el momento de la creación de éste.

Así pues, Bebo presenta problemas de privacidad importantes y no permite a los usuarios gestionar la co-propiedad de los álbumes que no les pertenecen, pudiendo darse grandes fugas de información en escenarios como el Escenario 2.

2.1.2 LinkedIn

LinkedIn es una red social orientada al mundo laboral, en la que los usuarios pueden indicar su formación académica y su trayectoria profesional. En ella se permite que los usuarios mantengan una lista de contactos con los que tienen alguna relación. Los usuarios pueden invitar a cualquier persona a unirse a relación. [7]

A pesar de las grandes ventajas que LinkedIn ofrece a nivel profesional, no es una red social dedicada a la compartición de imágenes, pudiendo cargar al sistema únicamente una imagen de perfil. No existe el concepto de etiqueta en esta red social, por lo tanto no hay ni puede haber gestión de co-propiedad alguna asociada a las fotos. Cuando se sube una imagen de perfil, se ofrecen tres opciones de visibilidad de ésta: pública, donde cualquier usuario puede ver esa imagen, "mi red", donde únicamente los usuarios que pertenezcan a los grupos del usuario podrán visualizar la imagen, y "mis contactos", donde los únicos usuarios que podrán ver la imagen serán los que el usuario tenga en su lista de contactos. [7]

En este caso no es posible generar escenarios ya que la única opción de privacidad permitida es la anteriormente citada y es asociada únicamente a la imagen de perfil de un único usuario.

2.1.3 Twitter

Twitter es una red social que permite a los usuarios enviar mensajes de texto de hasta 140 caracteres que posteriormente se muestran en las páginas principales de sus seguidores, que son usuarios que han decidido suscribirse a la cuenta de otro con el fin de que los mensajes que este último escriba se les muestre a ellos en su página principal. El sistema permite embeber contenidos multimedia en estos mensajes, llamados tweets, lo que incluye por lo tanto a las imágenes. No es posible crear álbumes de fotos ni etiquetar a las personas en las fotos como tal, pero sí que se permite "mencionar" a los demás usuarios en cualquier tweet mediante la expresión "@<nombre>", donde "nombre" es el nombre de un usuario, que éste ha elegido como identificador de su perfil. [8]

Atendiendo a la privacidad que ofrece Twitter, se puede elegir que los tweets estén protegidos, es decir, que únicamente los seguidores aprobados por el usuario podrán leer los tweets. En ningún caso se ofrecen herramientas específicas para la privacidad de las imágenes.

En cuanto a la gestión de la co-propiedad en las imágenes, se ha creado un escenario para las pruebas.

2.1.3.1 Escenario 1

En este escenario se tienen dos usuarios, "Álvaro", identificado por "@PruebasProyecto", y "Juan", identificado por "@PruebasProy2". Según la filosofía de Twitter, da igual que sean seguidores del otro o no para la gestión de las imágenes, y que sus tweets sean privados o no sólo influye en que lo leerán únicamente los seguidores del que ha publicado el tweet.

Seguidamente "Álvaro" publica una imagen donde menciona a "Juan". La imagen es visible por todo el mundo o, en el caso de tener su cuenta protegida, por todos sus seguidores. Desde la vista de "Juan" no se ofrecen herramientas para gestionar la co-propiedad de la imagen, siendo el último recurso disponible el de reportar el archivo mediante el hipervínculo de la esquina inferior derecha (Figura 6).

Figura 6. Imagen Twitter

2.1.4 Myspace

Myspace es una red social que permite la interconexión de personas unidas por una misma afición. Es una red social orientada a la música, donde los usuarios pueden subir sus canciones o sus álbumes completos para que otros usuarios puedan escucharlos.

La privacidad se define de forma parecida a otras redes sociales, donde el usuario puede decidir que su perfil sea público o restringido. Si se decide elegir el perfil público cualquier usuario podrá visualizarlo, incluyendo las fotos que se hayan subido, mientras que si se elige el perfil privado solamente podrán visualizar el perfil los usuarios que estén conectados a éste ("conexión" equivale a ser "amigos" en otras redes sociales). [9]

Myspace permite la subida de imágenes individuales, pero no existe el concepto de etiqueta de usuarios. Los usuarios pueden conectarse a las imágenes de otros, teniendo así un concepto parecido al de etiqueta. Por tanto, se definirán a continuación varios escenarios de pruebas para testear las políticas de gestión de la co-propiedad de las imágenes en esta red social.

2.1.4.1 Escenario 1

Se tienen dos usuarios: "Alvaro Galan", cuyo perfil es restringido y posee una imagen, y "Ags Ags", cuyo perfil es público. Ambos están conectados entre sí, por lo tanto "Ags Ags" tiene acceso a todo el perfil de "Alvaro Galan". "Ags Ags" decide

conectarse a la imagen que el otro posee, apareciendo ésta de esta forma visible en su perfil. (Figura 7)

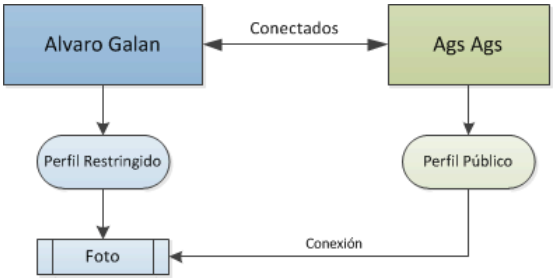

Figura 7. Escenario 1 Myspace

Aparece ahora un tercer usuario, "Juan", identificado mediante el nombre en Myspace "Pruebas Proyecto", el cual busca al usuario "Ags Ags" y, como tiene su perfil público, puede ver toda su información. Entre esta información, puede acceder a la sección de conexiones de fotos, donde, al ser el perfil de "Alvaro Galan" un perfil restringido, no se puede observar la imagen que posee "Alvaro Galan" que ha sido diseminada por "Ags Ags" en su perfil. El sistema no permite ni a "Alvaro Galan" ni a "Ags Ags" elegir la política de compartición de esta imagen. En la Figura 8 se puede observar cómo "Juan" no puede visualizar la imagen desde el perfil de "Ags Ags".

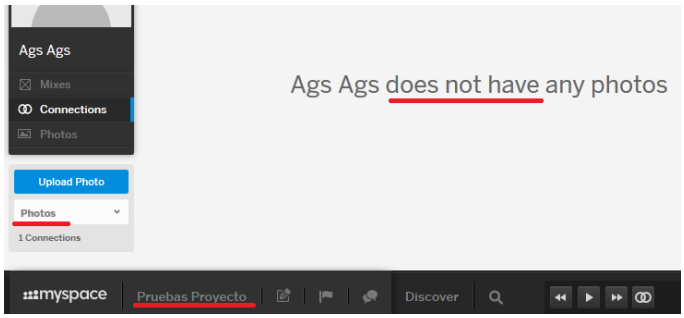

Figura 8. Vista Juan Myspace

2.1.4.2 Escenario 2

Se plantea ahora una situación muy parecida, donde es ahora "Ags Ags" el usuario que posee una imagen y "Alvaro Galan" quien está conectado a ella, supongamos porque aparece en ella. (Figura 9)

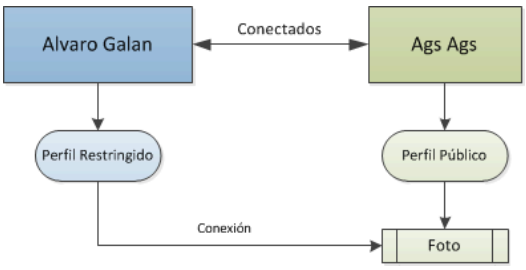

Figura 9. Escenario 2 Myspace

Nuevamente, aparece un tercer usuario, "Juan", identificado con el nombre "Pruebas Proyecto" en Myspace, que encuentra a "Ags Ags" en esta red social y decide

observar sus imágenes. En este caso sí que es capaz de visualizar la imagen donde además se puede apreciar la conexión a ella que ha hecho "Alvaro Galan". De igual forma, el sistema no permite ni a "Ags Ags" ni a "Alvaro Galan" decidir sobre la política de compartición de esta imagen, produciéndose de esta manera una fuga de información.

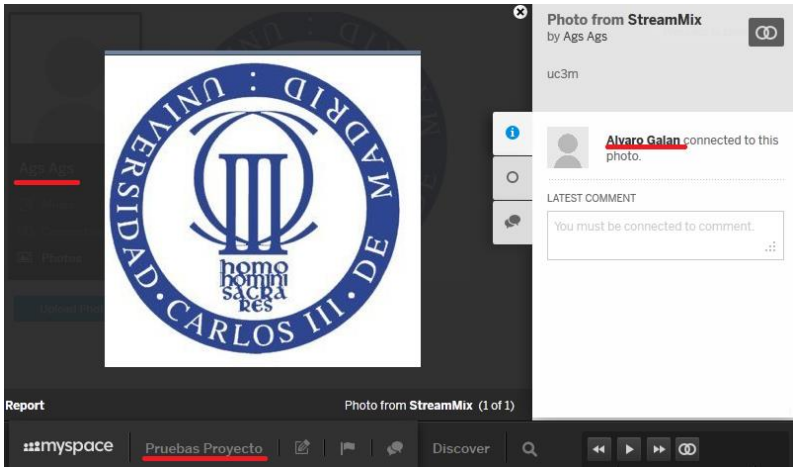

Figura 10. Escenario 2 Myspace

2.1.5 Facebook

Facebook es la red social por excelencia. Fue lanzada en 2004 para interconectar a los alumnos de la Universidad de Harvard y fue extendiéndose rápidamente a otras universidades para posteriormente dar el salto a interconectar a cualquier persona que lo desee. Esta red social permite la subida de álbumes de imágenes entre muchos otros contenidos.

La privacidad de las publicaciones se puede definir de forma predefinida, pudiendo elegir cuáles usuarios pueden verlas y cuáles no. Se pueden escoger varias políticas de control de acceso, siendo las más usuales "Público", "Amigos" (que incluye a los amigos de los usuarios involucrados) y "Solo yo". Se puede definir también la política de compartición para que únicamente los usuarios que pertenezcan a un grupo puedan visualizarlas.

La política que se escoja se aplicará por defecto a todas las publicaciones que el usuario haga, pero posteriormente se puede definir una política de compartición particular para cada una de ellas, dando así al usuario un gran control sobre qué información es visible por quién.

Atendiendo a la privacidad sobre los álbumes de imágenes, puede personalizar aún más la privacidad si se elige "Personalizado", donde se abre una ventana en la que se pueden controlar aspectos como que lo pueden ver los amigos de los usuarios etiquetados, los amigos de los amigos del usuario que posee el álbum o excluir a grupos o usuarios en concreto de verlo. [3]

A continuación se definirán una serie de escenarios para realizar pruebas sobre la gestión de la co-propiedad de los álbumes de imágenes.

2.1.5.1 . Escenario 1

Se tienen dos usuarios en Facebook, “Alvaro Galan”, que posee un álbum de imágenes con la privacidad fijada a “Amigos” en el que esta etiquetado otro usuario, “Ags Ags”, cuya política general de compartición es pública (Figura 11).

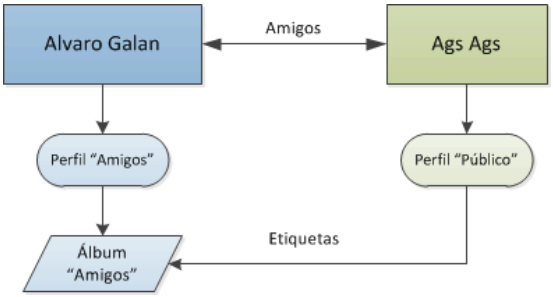

Figura 11. Escenario1 Facebook

De igual forma que se ha realizado en escenarios anteriores, aparece ahora un tercer usuario, llamado “Alvaro GS” que accede al perfil de “Ags Ags” e intenta visualizar sus imágenes. En este caso, el sistema no muestra imagen alguna. (Figura 12)

Figura 12. Fotos Ags Ags 1 Facebook

Facebook no posee ningún tipo de sistema de gestión de la co-propiedad ni a nivel de álbum ni a nivel de imagen individual, por lo que “Ags Ags” es incapaz de decidir la política de compartición, pudiendo únicamente escoger para cada foto individual si desea que se muestre en su biografía o no.

2.1.5.2 . Escenario 2

Se produce ahora una situación parecida, donde el dueño del álbum de fotos es ahora “Ags Ags”, que ha decidido que el álbum sea público, y “Alvaro Galan” es el usuario etiquetado en él. (Figura 13)

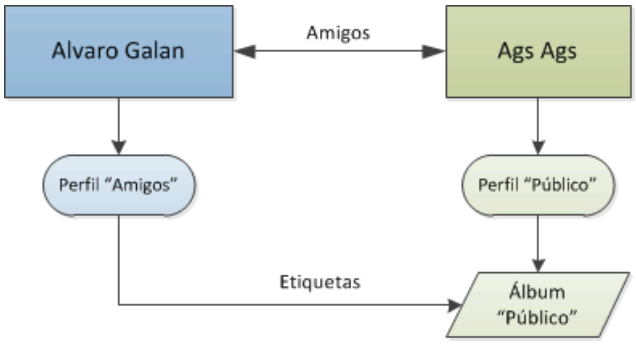

Figura 13. Fotos Ags Ags 1 Facebook

Nuevamente, el usuario "Alvaro GS" trata de acceder al perfil de "Ags Ags", pudiendo contemplar en este caso su álbum de fotos donde está involucrado "Alvaro Galan" (Figura 14).

Figura 14. Fotos Ags Ags 2 Facebook

El sistema no permite a "Alvaro Galan" gestionar la co-propiedad del álbum, por tanto se produce una fuga de información que podría no interesar a este usuario en ciertos casos. La única herramienta que se le da para controlar esto nuevamente es aprobar cada imagen o no para que aparezca en su biografía.

2.1.5.3 . Escenario 3

En este caso, se propone el mismo escenario que en el Escenario 1, diferenciándolo de él únicamente que en este caso, el usuario "Alvaro GS" es un amigo de "Ags Ags", teniendo el esquema que representa la Figura 15.

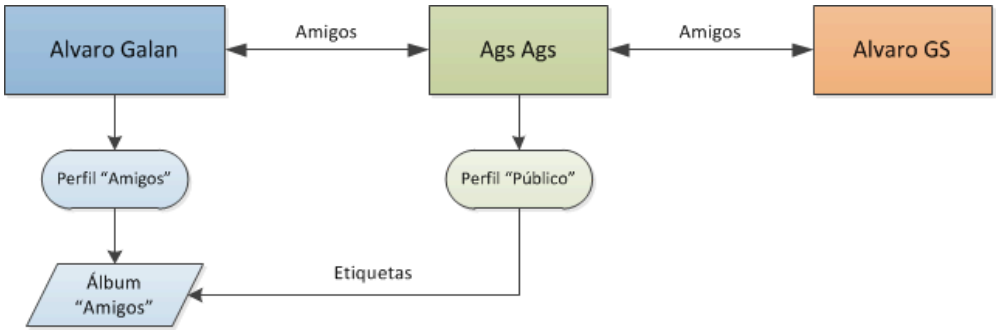

Figura 15. Escenario 3 Facebook

Es en este momento cuando el usuario "Alvaro GS" accede al perfil de "Ags Ags" para contemplar sus fotos. En este caso se pueden contemplar sin ningún problema, ya que la política "Amigos" incluye también a los amigos de las personas involucradas (Figura 16)

Figura 16. Fotos Ags Ags 3 Facebook

"Alvaro Galan", que es el propietario, puede decidir no compartir el álbum con los amigos de las personas involucradas, pero en ningún caso "Ags Ags" puede decidir una política de compartición ni a nivel de imagen ni a nivel de álbum.

Como conclusión al haber estudiado estas cinco redes sociales, se puede extraer que la fortaleza de la privacidad en algunas de ellas es mayor y más flexible que en algunas de otras, pero sobre todo que ninguna de ellas provee de un mecanismo de gestión de la co-propiedad que permita a los usuarios involucrados en cada foto o en cada álbum decidir quién puede visualizar el contenido o quién no.

2.1.6 Comparación

A continuación, se ha elaborado la Tabla 1, que representa un resumen de las características de las redes sociales estudiadas.

Red social	Subida de imágenes	Subida de álbumes	Etiqueta de otros usuarios	Gestión de la co-propiedad
Bebo	Sí	Sí	Sí	No
LinkedIn	Sí (perfil)	No	No	No
Twitter	Sí	No	Sí (mención)	No
Myspace	Sí	No	Sí (conexión)	No
Facebook	Sí	Sí	Sí	No

Tabla 1. Comparación redes sociales

Como se puede observar, de una forma u otra todas presentan características similares en cuanto a la subida de imágenes. No todas ellas permiten la subida de álbumes, quizá por el enfoque que presenta la red social ya que en algunos casos no se presenta como una necesidad. El concepto de etiqueta es muy parecido entre todas ellas, excepto en LinkedIn que, como únicamente permite la subida de fotos de perfil, no se considera este concepto. La problemática viene al observar la última columna, donde se puede apreciar que el único aspecto que ninguna de ellas cubre es el de la gestión de la co-propiedad, poniendo de esta forma en peligro la privacidad de los usuarios.

2.2 Líneas de investigación

Se ha realizado una búsqueda de artículos de investigación acerca de la gestión de la co-propiedad en las redes sociales. Tras esta búsqueda, se han encontrado diversos modelos de gestión que tratan de solventar la fuga de información sensible. Todos ellos coinciden en que estas fugas son debidas a que no existe una gestión de la co-propiedad más rigurosa. Es importante remarcar que todos ellos hacen referencia a contenidos en general, por lo que no se especifica que sea concretamente para fotos o álbumes de fotos.

2.2.1 Año 2010

En el año 2010 comienza a haber las aproximaciones más notables a los sistemas de gestión políticas de co-propiedad. En un artículo [10] se trata de diseñar un sistema de co-propiedad para contenidos en general, pero se detalla el caso de las fotos. Las potenciales partes interesadas, que serán los co-propietarios de la foto, se identifican gracias a metadatos, reconocimiento facial o por iniciativa del propietario. Se propone que el método más adecuado para aplicar la decisión sería que las partes implicadas votasen y, tras varias rondas de votaciones, llegasen a una política común. Además, el sistema tratará de facilitar a los usuarios la tarea de establecer una política sugiriéndoles la política de privacidad que desean mediante técnicas de inferencia. Esta propuesta presenta problemas muy similares a la anterior ya que los conjuntos de usuarios que podrán ver las imágenes podrían ser muy pequeños o incluso vacíos.

Un mes más tarde, en otro de los artículos [11] se propone un sistema de co-propiedad para contenidos en general donde todas las solicitudes para acceder a un recurso pasen por un "punto de decisión de política". Para poder elegir la política las partes interesadas deben estar dispuestas a colaborar con la definición de la política y cada una de ellas tiene derecho a restringir el acceso al recurso arbitrariamente a quien deseen. El mecanismo de autorización se basa en un funcionamiento simple: cualquier propietario o co-propietario puede añadir una política "débil" y una política "fuerte" o pueden eliminar una de las existentes. Las partes implicadas pueden negociar las políticas "débiles" pero pueden imponer restricciones no negociables, que serán las políticas "fuertes". El sistema puede ser ajustado para que se pueda decidir qué usuarios pueden imponer condiciones fuertes y cuales únicamente condiciones débiles. Es sencillo verificar que mediante este sistema pueden derivar en conflictos de intereses, donde no se satisfagan todas las condiciones de cada una de las partes implicadas. La solución a la resolución de estos conflictos se menciona, pero no se presentan mecanismos que puedan ayudar a resolver el problema. También se pueden producir situaciones de sabotaje entre los co-propietarios, donde uno de ellos podría imponer una política muy restrictiva. No se propone ningún mecanismo para detectar esta situación y la responsabilidad de lidiar con esta situación recae en los demás co-propietarios. Para ello sí se habilita un sistema de reporte de co-propietarios, pudiendo reelegir de nuevo la política o incluso excluir del contenido al co-propietario malicioso. Esta resolución de conflictos es demasiado restrictiva y pueden darse situaciones de conflicto para alguno de los co-propietarios ya que se les puede excluir de gestionar la co-propiedad.

2.2.2 Año 2011

En el año 2011 se presenta se presenta el sistema CoPE [12], que gestiona la co-propiedad para cualquier tipo de contenido donde las partes implicadas especifican sus preferencias de privacidad de forma anónima para los demás co-propietarios. Se definen específicamente estas políticas, que pueden ser: "algunos amigos", que son los usuarios que tienen algún tipo de relación específica con los implicados o los usuarios que éstos no quieren que tengan acceso al contenido, "público", que son todos los usuarios del sistema, tengan relación con los implicados o no, y "co-propietarios solo", que permite únicamente a las partes implicadas visualizar el contenido. Una vez cada uno de los implicados ha realizado su voto, el sistema agrupa y contabiliza las preferencias de privacidad. Sólo los usuarios que intersecccionen entre las preferencias establecidas tendrán acceso al contenido. Por último, cada vez que se añada una parte interesada se añadirá su política de privacidad y se volverá a computar el conjunto de usuarios que tienen acceso al contenido. En definitiva, está técnica preserva la privacidad de todos los usuarios pero es altamente restrictiva. Pueden darse casos de conjuntos vacíos o de muy pocos usuarios con permiso a acceder al contenido, lo que en sí es excesivamente restrictivo.

2.2.3 Año 2012

En año 2012 se proponen en un mismo artículo varios sistemas aplicados en el establecimiento de políticas de propietarios y co-propietarios: un sistema de votos donde la decisión final de la política puede ser tomada en base a dos esquemas, un sistema basado en umbral y un sistema basado en estrategia de resolución de conflictos, donde la decisión final puede ser tomada mediante tres esquemas [13].

El sistema de votos basado en "decisión" propone que el voto de todos los implicados en el contenido tenga el mismo valor y que este voto sea binario, es decir, "permitir" o "no permitir". Finalmente se obtiene un valor entre cero y uno que será la media de las votaciones. Este esquema es bastante inflexible, ya que la decisión individual es binaria. El segundo esquema de votos es el basado en "sensibilidad", donde, en una escala de cero a uno, cada parte implicada asigna un valor de sensibilidad a ese contenido, que se corresponde con su política de privacidad elegida. El sistema basado en umbral toma de base el sistema de votos y le añade el factor de la toma de decisión. Este sistema permite controlar con mayor precisión la fuga de informaciones. El sistema basado en estrategia de resolución de conflictos propone tres esquemas para la toma de la decisión final. El primero de ellos es un esquema donde el propietario del contenido tiene el control total sobre la decisión de la política, por lo que no se permite que los demás implicados voten. El segundo esquema propone que la decisión sea unánime y por tanto se considera que es un sistema restrictivo. El último esquema propone que la mayoría decida el acceso.

Aún con estos tres sistemas complementarios existen carencias a cubrir ya que las situaciones de conflicto pueden llegar a ser injustas para algunos de los co-propietarios gracias a los votos de otros.

2.2.4 Discusión

Como conclusión tras realizar esta investigación sobre trabajos acerca de la gestión de la co-propiedad, se puede determinar que los artículos [10] y [11] fueron una primera aproximación a un sistema de gestión de las políticas pero que hoy día no son lo suficientemente adecuados. El artículo [12] propone un sistema mucho más granular y equitativo, aunque sigue teniendo carencias en las situaciones conflictivas. Finalmente el artículo [13] propone una solución más satisfactoria que las anteriores, puesto que se proponen varios sistemas de votaciones, de decisión y de resolución de conflictos, pero siguen existiendo carencias necesarias de cubrir.

Capítulo 3

Análisis

3.1 Perspectiva general del sistema

En esta sección se describe el sistema a implementar para garantizar los dos objetivos definidos en el Capítulo 1 del presente documento: desarrollar una aplicación que permita establecer de forma cooperativa una política de control de acceso a un álbum y garantizar el acceso anónimo al álbum mediante el uso de una credencial.

Para garantizar el primero de ellos, el sistema debe apoyarse en un mecanismo de votación donde los co-propietarios introducirán sus preferencias de control de acceso al álbum. Esta votación se debe realizar de forma anónima, por lo que ningún co-propietario debe conocer las preferencias que los demás usuarios han introducido. Tampoco debe existir ningún medio físico o técnico que permita averiguar las preferencias concretas de cualquiera de los co-propietarios. Debido a que no existen implementaciones prácticas de este tipo de sistema, deberá realizarse el desarrollo de uno propio.

Para garantizar el segundo de los objetivos, se aplicará un sistema de credenciales anónimas que facilite a los usuarios el acceso en base a atributos que ellos posean y que están incluidos dentro de una credencial.

La red social escogida como plataforma sobre la que realizar la implementación es Facebook ya que su API ofrece diversas opciones útiles para el manejo de álbumes de manera externa. Los datos obtenidos de ella servirán como base para obtener la información relevante para el sistema. Por tanto, el sistema debe ser una aplicación real de Facebook y deben poderlo utilizar los usuarios desde la propia red social.

3.2 Arquitectura del sistema

Debido a la las partes diferenciadas del sistema, se ha decidido realizar un diseño modular donde la funcionalidad de cada uno de los componentes queda totalmente definida y separada de la de los demás.

En la Figura 17 se muestra el diagrama de componentes inicial de la arquitectura del sistema. Se ha utilizado el patrón de diseño MVC, donde se ha separado la lógica de negocio de los datos y de la interfaz. Dentro de un mismo componente llamado sistema, se encuentran los componentes que componen el núcleo de la aplicación. En él se encuentran los correspondientes a la votación realizada por los co-propietarios, el control de acceso a los álbumes mediante el uso de una credencial, la interfaz de usuario y la base de datos donde se deberá almacenar información relativa a los procesos de votación.

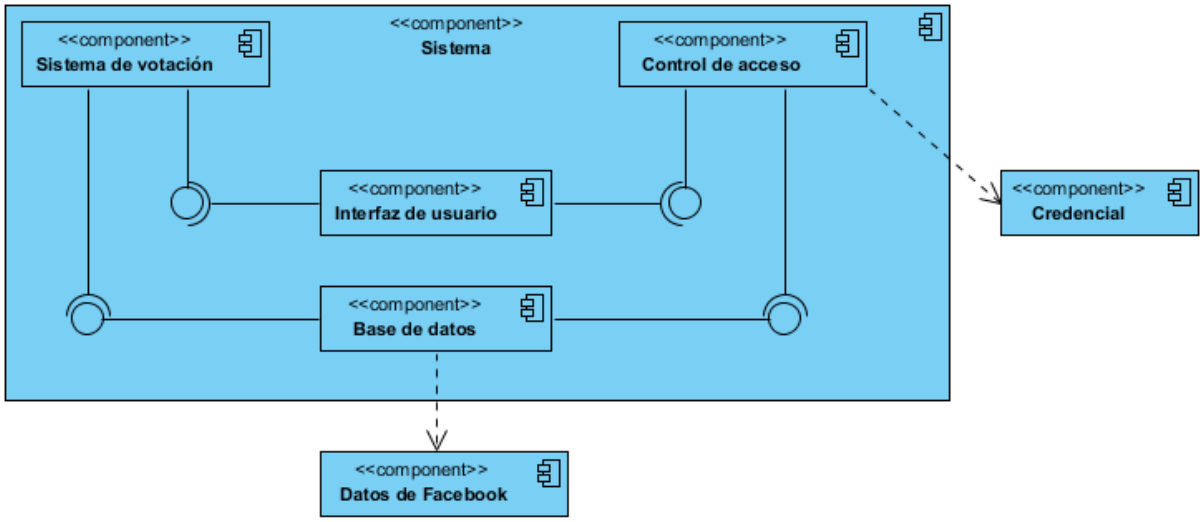

Figura 17. Arquitectura inicial

De forma externa al sistema, se encuentran dos componentes más. Uno de ellos representa los datos que deben ser obtenidos de Facebook para poder realizar las votaciones sobre los álbumes. El otro representa las credenciales anónimas usadas para acceder a visualizar los álbumes de fotografías que se hayan compartido previamente en el sistema.

3.3 Estudio tecnológico

En esta sección se realiza el estudio de las tecnologías que se pueden aplicar para la implementación de los diversos componentes que forman la aplicación. En las siguientes subsecciones se analizan las tecnologías impuestas y las tecnologías aplicables a los distintos componentes definidos en la arquitectura inicial.

3.3.1 Tecnologías impuestas

Existe una restricción tecnológica a la hora de obtener los datos de Facebook, ya que esta red social ofrece cuatro kits de desarrollo de software (SDK). Las tecnologías sobre las que ofrece estos SDK son Android [14], iOS [15], PHP y JavaScript [16]. Debido a que se quiere asegurar una máxima portabilidad, los dos primeros han sido descartados ya que obligaría a los usuarios a disponer de un sistema que utilizara Andoid o iOS y se orienta, por lo tanto, el sistema a trabajar sobre tecnologías web. Por este mismo motivo, el componente de la interfaz de usuario deberá utilizar la tecnología HTML como base sobre la que fundamentarse.

La otra de las restricciones se centra en el componente credencial, del cual se dispone de sistemas básicos de generación y comprobación de las credenciales, que deberán ser adaptados posteriormente y que utilizan la tecnología Java.

3.3.2 Tecnologías aplicables al componente *Sistema de votación*

Este componente se encargará de hacer efectivas las votaciones de las políticas de control de acceso para los álbumes. Para ello se requiere una tecnología que trabaje las herramientas matemáticas con facilidad y modularidad, ya que las votaciones en sí consistirán en realizar operaciones matemáticas sobre ciertos valores para enmascarar las preferencias de los usuarios. También se requiere la máxima compatibilidad con las tecnologías web. Tras estas premisas, las tecnologías estudiadas para este componente son C++, Java, JavaScript y PHP.

La primera tecnología a analizar es C++. Esta tecnología está orientada a objetos y, por lo tanto, ofrece una modularidad adecuada a las necesidades del sistema. Existen también librerías y herramientas matemáticas que puedan permitir la manipulación de los datos necesarios sin ningún tipo de problema. Sin embargo, no presenta una compatibilidad suficiente con las tecnologías web, ya que C++ ofrece una buena compatibilidad con los servicios web pero no con los servidores ni las páginas web. [17]

La segunda tecnología estudiada es Java. Esta tecnología, al igual que la anterior, está orientada a objetos y su modularidad es óptima. Las herramientas matemáticas

existentes para Java son diversas y se encuentran con gran facilidad, por lo tanto este aspecto está también completamente cubierto por esta tecnología. En primera instancia, Java presenta el mismo problema que C++ respecto a las tecnologías web, pero existen diversos servidores web que trabajan con esta tecnología como base sobre la que ejecutar el código de la máquina servidora. Esto es una gran ventaja pero, a su vez, no permite la ejecución de código en las máquinas clientes de los usuarios, ya que por motivos de seguridad será necesario realizar cálculos localmente en estas máquinas. [18]

La tercera tecnología revisada es JavaScript. Se trata de una tecnología que trabaja únicamente en entornos web, así pues el aspecto de la compatibilidad web está cubierto por completo. La capacidad matemática de esta tecnología es similar a la que ofrece la tecnología de la cual deriva (Java), pero las librerías matemáticas son menos frecuentes para JavaScript. La modularidad es aceptable, ya que es posible separar las funcionalidades necesarias con facilidad. Esta tecnología trabaja localmente en la máquina del usuario, por lo que cubre las necesidades de seguridad comentadas anteriormente. [19]

Por último, se ha estudiado PHP. Esta tecnología es exclusiva para entornos web y por tanto es compatible con el requisito impuesto. La capacidad matemática es aceptable, pero no lo es tanto la existencia de librerías. En lo que a modularidad se refiere, no ofrece una modularidad suficiente para las diferentes funcionalidades del sistema. [20]

3.3.3 Tecnologías aplicables al componente *Control de acceso*

Este componente se encarga de realizar las comprobaciones necesarias sobre una credencial para determinar si el usuario puede acceder o no al álbum. Para hacer esto posible se requiere una tecnología que ejecute una comprobación en la máquina local del usuario, asegurando así la privacidad de la credencial, así como una comprobación en la máquina servidora para verificar la comprobación realizada en local por el usuario. Nuevamente se requieren tecnologías con un componente matemático muy fuerte y la máxima portabilidad. Las tecnologías analizadas son C++ y Java.

La primera de ellas, como ya se ha mencionado anteriormente, dispone de herramientas matemáticas consolidadas y potentes, así como librerías de apoyo, por lo que este aspecto queda cubierto. Sin embargo, C++ requiere de un compilador instalado en la máquina cliente, aspecto que no es muy usual en un usuario normal del sistema. Por último, tal como se comentó en la sección anterior, no presenta una gran compatibilidad con los entornos de servidores de aplicaciones.

Java, al igual que C++, dispone de una gran potencia matemática y de un amplio abanico de librerías de apoyo [21], por lo tanto este aspecto queda igualmente cubierto. En el aspecto de portabilidad, Java fue creado con el propósito de ejecutarse bajo cualquier entorno, usando para ello máquinas virtuales (JVM) sobre las que se ejecuta la aplicación, por lo tanto la portabilidad es máxima. [18] De igual forma que se comentó en la sección anterior, Java soporta los entornos de servidores de aplicaciones a la perfección, ya que es la tecnología base de varios de los más relevantes. [22] [23]

3.3.4 Tecnologías aplicables al componente *Base de datos*

Este componente representa la base de datos que será necesaria para almacenar los datos relevantes para el sistema. Existen varios modelos de bases de datos, pero el que más se ajusta a las necesidades del sistema es el relacional, ya que permite establecer interrelaciones entre las distintas tablas. Las tecnologías estudiadas son Oracle y MySQL.

La primera de ellas pertenece a la empresa que lleva su mismo nombre y se caracteriza por ser un sistema de bases de datos muy completo y que ofrece características como soporte de transacciones, estabilidad, escalabilidad y soporte multiplataforma. Los requerimientos del sistema están cubiertos perfectamente con esta tecnología. A pesar de las ventajas que ofrece, uno de los grandes inconvenientes es que es un producto de pago. [24]

MySQL pertenece también a la empresa Oracle, pero es un producto de software libre y, por tanto, gratuito. Ofrece características relevantes como soporte de transacciones, conectividad segura y soporte multiplataforma. Para los requerimientos del sistema, cumple a la perfección su función. [25]

3.3.5 Tecnologías aplicables al componente *Datos de Facebook*

Este componente se encarga de obtener los datos reales de los usuarios de la red social Facebook. Esto se debe realizar mediante el SDK de JavaScript o el de PHP. Ya que las características que ofrecen ambos SDK son idénticas, el único factor a analizar es la máxima modularidad y la adaptabilidad de estos lenguajes con las demás tecnologías.

Por norma general, se puede utilizar JavaScript en cualquier entorno web, ya que el código es interpretado por el propio navegador del usuario y no se depende de ningún servicio externo. Por este motivo la adaptabilidad que ofrece JavaScript es muy alta. [26]

En el caso de PHP se requiere la mediación de un servidor PHP para que sea posible ejecutar esta tecnología. La adaptabilidad que ofrece en este caso sólo sería buena si se escogiese implementar todo el sistema bajo esta tecnología, ya que el sistema presenta restricciones si se deseara combinar esta tecnología con otras. [27]

3.4 Selección de tecnologías no impuestas

En esta sección se seleccionarán las tecnologías propuestas anteriormente para cada componente, siempre intentando maximizar la interconexión entre cada uno de ellos.

En primer lugar, se ha decidido utilizar un servidor web Apache Tomcat, que fundamenta su base sobre código Java, para así maximizar la compatibilidad entre cada uno de los componentes ya que será la tecnología base, con pequeños matices diferenciadores, para todos ellos.

La tecnología seleccionada para el sistema de votación, sección 3.3.2, será una combinación entre JavaScript y la parte servidora que ofrece Tomcat en Java. Parte del cómputo requiere ser realizado de forma local para asegurar la privacidad de los usuarios, es por esto que esta parte será realizada por JavaScript. Otra parte del cómputo requiere ser procesada y almacenada en el servidor web, de lo cual se encarga la tecnología Java. Se ha descartado utilizar C++ por los inconvenientes de compatibilidad web que presenta. También se ha descartado la opción de utilizar PHP por su baja modularidad y la falta de acoplamiento con otras tecnologías.

Se ha seleccionado la tecnología Java para el componente del control de acceso, sección 3.3.3, debido a que de esta forma se maximiza la portabilidad del módulo que el cliente debe ejecutar en su máquina y también se facilita la integración de la parte servidora en Tomcat. Por este mismo motivo de integración ha sido descartada la tecnología C++.

La tecnología usada para las bases de datos, sección 3.3.4, es MySQL. Si bien es cierto que los resultados son más satisfactorios usando Oracle, con el fin de abaratar los costes finales del proyecto, se ha decidido usar esta alternativa de software libre que solventa a la perfección las necesidades establecidas.

Finalmente se ha escogido JavaScript como tecnología para obtener los datos de Facebook, sección 3.3.5. El motivo es su gran portabilidad y la compatibilidad con las tecnologías escogidas para la implementación del sistema.

3.5 Arquitectura definitiva de alto nivel

Una vez consideradas las selecciones tecnológicas del sistema, se ha elaborado una arquitectura definitiva a partir de la arquitectura inicial considerada en la sección 3.2. De igual forma que en la sección 3.2, se ha utilizado el patrón de diseño MVC para componer la arquitectura definitiva del sistema, donde se separa la lógica de negocio de los datos y de la interfaz. En esta arquitectura se refleja la necesidad de separar el sistema en dos componentes, cliente y servidor, debido a las decisiones tecnológicas adoptadas.

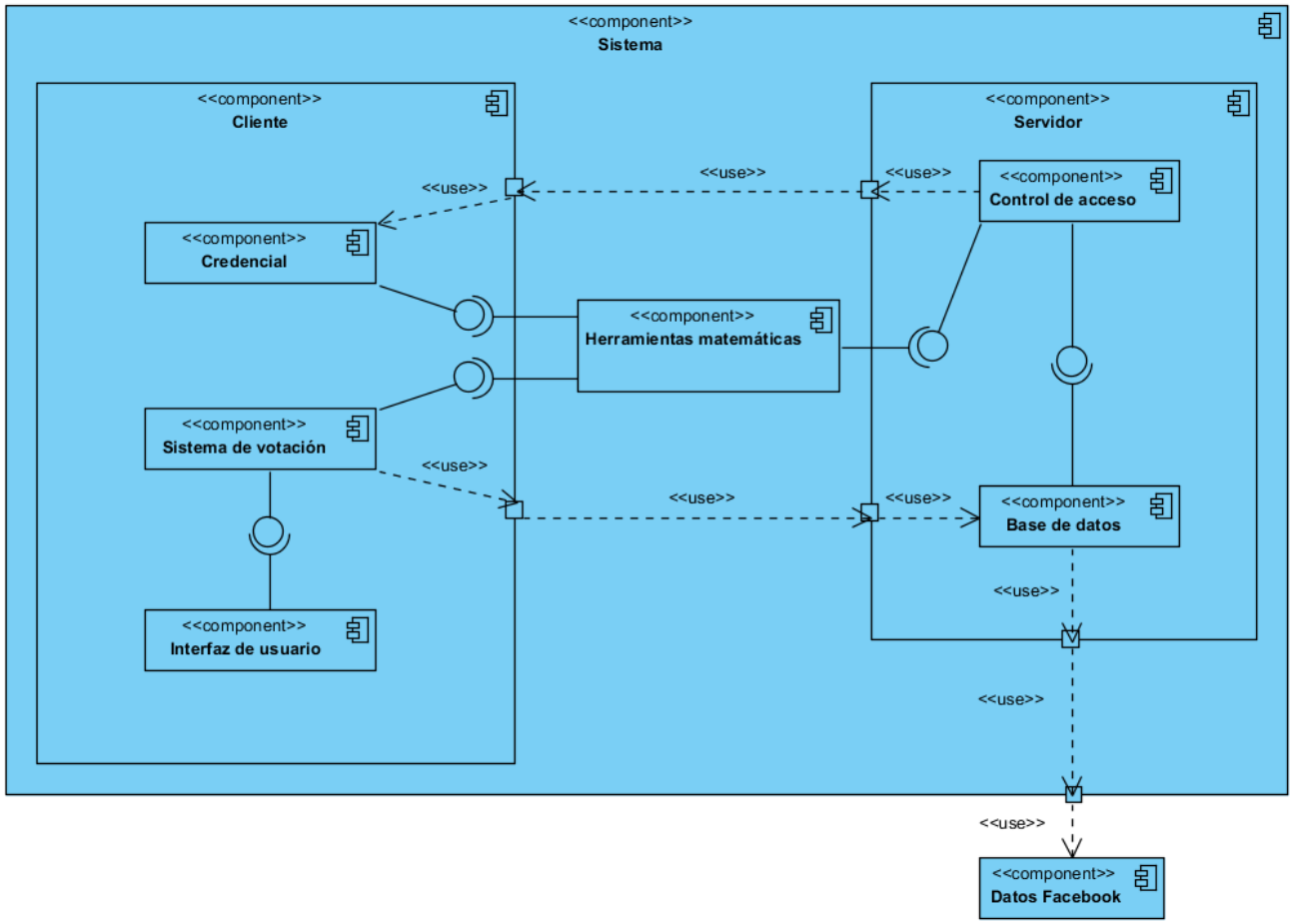

Figura 18. Arquitectura definitiva de alto nivel

En primer lugar, existe un gran componente que agrupa a todos los demás (excepto a los datos de Facebook), el cual recibe el nombre de “sistema” y es considerado el núcleo de la aplicación. En el componente cliente se agrupa la funcionalidad que deberá tener el módulo desarrollado para hacer cómputos en la máquina local. Es por ello que contiene al sistema de votación entre los co-propietarios y a la funcionalidad asociada a la credencial anónima, ya que, como se ha comentado, los cálculos asociados a estos dos componentes deben ser realizados de forma local por motivos de seguridad. La interfaz de usuario también está contenida en el cliente ya que será éste quien visualice el sistema para la votación.

El componente servidor agrupa la funcionalidad del control de acceso, donde se realizarán las comprobaciones necesarias sobre una credencial para verificar si cumple la política. También engloba la funcionalidad del almacenaje de los datos necesarios, para lo cual se dispone de un puerto de acceso a los datos reales de Facebook, que son un componente externo al sistema y queda reflejado como tal en el diagrama.

Por último, se dispone de un componente que usan ambos componentes principales: las herramientas matemáticas. Aquí se engloban el conjunto de librerías y herramientas necesarias para hacer posible la votación y la comprobación y generación de las credenciales.

3.6 Casos de uso

En esta sección se define el diagrama de casos de uso junto con sus definiciones textuales en sus correspondientes subsecciones. A partir de ellos será posible extraer los requisitos de software.

3.6.1 Diagrama de casos de uso

Se ha elaborado el diagrama de casos de uso con el fin de diferenciar las funcionalidades del sistema. En este caso, se han identificado tres casos de uso diferentes. El primero de ellos se corresponde con el caso de uso CU-01, el cual hace referencia al momento en el que el propietario de un álbum decide compartirlo y para ello escoge a los co-propietarios y selecciona las preferencias propias. El caso de uso CU-02 representa la funcionalidad referente al momento en el que un co-propietario introduce sus preferencias para un álbum que alguien ha decidido compartir con él. En el caso de uso CU-03, un usuario decide acceder a visualizar un álbum previamente compartido, para lo cual se deberá chequear si posee permiso para hacerlo.

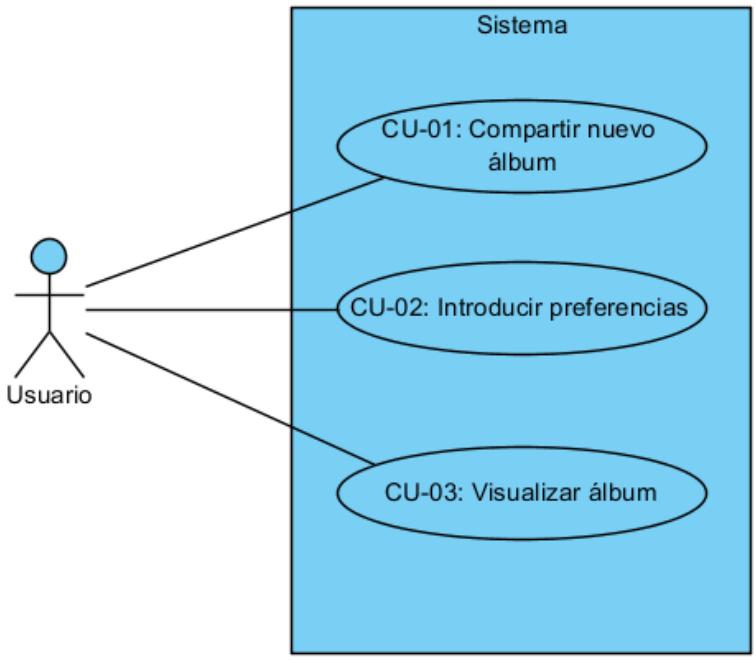

Figura 19. Diagrama de casos de uso

3.6.2 Definición textual de los casos de uso

A continuación se mostrará la definición de cada caso de uso de forma detallada en su correspondiente tabla.

La siguiente tabla muestra el caso de uso CU-01, que representa la acción de un usuario, propietario de un álbum de fotos en Facebook, que desea decidir la política de control de acceso al álbum de forma conjunta con el resto de los co-propietarios. Para ello debe seleccionar a los co-propietarios de éste y elegir sus preferencias de privacidad.

Id: CU-01	
Nombre:	Compartir nuevo álbum
Autor:	Álvaro Galán Serrano
Descripción: Compartir un nuevo álbum de fotos de Facebook con el fin de elegir la política de control de acceso de forma conjunta con los demás co-propietarios.	
Actores: Usuario propietario del álbum a compartir.	
Precondiciones: • El usuario debe estar logueado en Facebook. • El usuario debe poseer un álbum en Facebook. • El usuario debe poseer al menos un amigo en Facebook.	
Poscondiciones: • El usuario ha debido seleccionar sus preferencias de privacidad para el álbum. • Los co-propietarios han debido ser notificados de que el propietario quiere decidir la política de control de acceso al álbum conjuntamente.	
Flujo normal: 1. Seleccionar el álbum que se desea compartir. 2. Seleccionar los amigos co-propietarios del álbum. 3. Seleccionar las preferencias de privacidad. 4. Notificar a los demás co-propietarios. 5. Finalizar.	
Flujo alternativo: 2a. El usuario decide compartir otro álbum. 3a. Ir al paso 1. 3b. El usuario decide seleccionar otros amigos co-propietarios. 4b. Ir al paso 2. 4c. El usuario decide seleccionar otras preferencias de privacidad. 5c. Ir al paso 3.	

Tabla 2. Caso de uso CU-01

La siguiente tabla muestra el caso de uso CU-02, que representa la acción de un usuario, co-propietario de un álbum de fotos en Facebook, al que se ha notificado que se desea decidir la política de control de acceso a éste de forma conjunta. Para ello debe elegir sus preferencias de privacidad utilizando el sistema.

Id: CU-02	
Nombre:	Introducir preferencias
Autor:	Álvaro Galán Serrano
Descripción: Seleccionar las preferencias de control de acceso a un álbum de fotos de Facebook con el fin de elegir la política de control de acceso de forma conjunta con los demás co-propietarios.	
Actores: Usuario co-propietario del álbum a compartir.	
Precondiciones: • El usuario debe estar logueado en Facebook. • El usuario debe haber sido notificado por el propietario de un álbum de Facebook para que introduzca sus preferencias.	
Poscondiciones: • El usuario ha debido seleccionar sus preferencias de privacidad para el álbum.	
Flujo normal: 1. Seleccionar las preferencias de privacidad. 2. Finalizar.	
Flujo alternativo: 2a. El usuario decide seleccionar otras preferencias de privacidad. 3a. Ir al paso 1.	

Tabla 3. Caso de uso CU-02

La siguiente tabla muestra el caso de uso CU-03, que representa la acción de un usuario que desea acceder de forma anónima a visitar un álbum de fotos de Facebook previamente compartido en el sistema. Para ello chequearse su permiso mediante una credencial.

Id: CU-03	
Nombre:	Visualizar álbum
Autor:	Álvaro Galán Serrano
Descripción: Acceder a visualizar un álbum de fotos de Facebook previamente compartido en el sistema.	
Actores: Usuario del sistema.	
Precondiciones: • El usuario debe poseer una credencial.	
Poscondiciones: • El usuario ha accedido, o no, a visualizar el álbum seleccionado.	
Flujo normal: 1. Seleccionar el álbum que se desea visualizar. 2. Presentar la credencial al sistema. 3. Visualizar el álbum. 4. Finalizar.	
Flujo alternativo: 3a. El sistema comprueba que el usuario no tiene permiso para acceder al álbum. 4a. Ir al paso 1.	

Tabla 4. Caso de uso CU-03

3.7 Requisitos de software

En esta sección se encuentran los requisitos de software extraídos tras el análisis del sistema. A continuación, en las siguientes subsecciones, se describirán los requisitos funcionales y los no funcionales.

3.7.1 Requisitos funcionales

En la siguiente tabla se muestran los requisitos funcionales del sistema.

Requisitos de Software				
Tipo: Funcional				
Id	**Nombre**	**Descripción**	**Estabilidad**	**Prioridad**
RF-01	Aplicación web.	El sistema implementado debe ser una aplicación web.	Alta	Alta
RF-02	Aplicación de Facebook.	El sistema implementado debe ser una aplicación de Facebook.	Alta	Alta
RF-03	Sistema cliente-servidor.	El sistema debe seguir la arquitectura cliente-servidor utilizada en las aplicaciones web.	Alta	Alta
RF-04	Navegación segura.	La navegación web debe realizarse de manera cifrada mediante SSL.	Alta	Alta
RF-05	Compartición de álbumes.	El sistema debe permitir al propietario de un álbum de fotos de Facebook compartirlo desde la aplicación.	Alta	Alta
RF-06	Votación.	El sistema debe permitir realizar una votación de la política de control de acceso para los álbumes.	Alta	Alta
RF-07	Política de control de acceso 1.	La política de control de acceso al álbum votado será computada cuando todos los co-propietarios hayan seleccionado sus preferencias.	Alta	Alta
RF-08	Política de control de acceso 2.	La selección de cada preferencia en la política de control de acceso será realizada como la opción más votada por los co-propietarios.	Media	Media
RF-09	Anonimato en la votación.	El sistema debe realizar los cómputos en la máquina cliente para asegurar el anonimato y la privacidad en la votación.	Alta	Alta
RF-10	Selección de amigos.	El sistema debe permitir al propietario de un álbum seleccionar los amigos co-propietarios con quien desea acordar una política de acceso conjunta.	Alta	Alta

Requisitos de Software				
Tipo: Funcional				
Id	**Nombre**	**Descripción**	**Estabilidad**	**Prioridad**
RF-11	Notificación.	El sistema debe notificar mediante un mensaje de Facebook, en nombre del propietario, a los co-propietarios de un álbum de que se requiere su intervención en la aplicación.	Media	Alta
RF-12	Lista de álbumes.	El sistema debe permitir acceder a la lista de álbumes previamente compartidos en el sistema.	Alta	Alta
RF-13	Chequeo de credenciales.	El sistema debe chequear la credencial del usuario que intente acceder a visualizar un álbum.	Alta	Alta
RF-14	Anonimato en el chequeo.	El sistema debe realizar los cómputos en la máquina cliente para asegurar el anonimato y la privacidad en el chequeo de las credenciales.		
RF-15	Denegación de acceso.	El sistema debe denegar el acceso a la visualización de un álbum cuando el chequeo de la credencial haya sido erróneo.	Alta	Alta
RF-16	Acceso positivo.	El sistema debe permitir el acceso a la visualización de un álbum cuando el chequeo de la credencial haya sido correcto.	Alta	Alta
RF-76	Privacidad de los datos.	El sistema no debe recopilar ningún dato que sea de carácter privado en ninguno de sus usos.	Alta	Alta

Tabla 5. Requisitos funcionales

3.7.2 Requisitos no funcionales

En la siguiente tabla se muestran los requisitos no funcionales del sistema.

Requisitos de Software				
Tipo: Interfaz				
Id	**Nombre**	**Descripción**	**Estabilidad**	**Prioridad**
RNF-01	Funcionalidades.	El sistema debe mostrar las funcionalidades disponibles.	Media	Media
RNF-02	Lista de álbumes.	El sistema debe mostrar una lista de los posibles álbumes a los que se pueden acceder.	Alta	Alta
RNF-03	Color.	El tema de la aplicación deberá seguir el estilo de Facebook.	Baja	Baja
RNF-04	Diseño de la aplicación.	El diseño de la aplicación debe mantenerse entre cada pantalla.	Alta	Alta
Tipo: Operacional				
Id	**Nombre**	**Descripción**	**Estabilidad**	**Prioridad**
RNF-05	Idioma.	El idioma utilizado en el sistema será el inglés.	Media	Media
RNF-06	Mensajes de información.	El sistema utilizará mensajes de información explicativos en cada una de las pantallas.	Alta	Alta
RNF-07	Mensajes de error.	El sistema utilizará mensajes de error en el caso de producirse uno.	Alta	Alta
RNF-08	Validación de los datos.	El sistema debe validar los datos introducidos por el usuario en los formularios.	Alta	Alta

Tabla 6. Requisitos no funcionales

3.8 Diseño del plan de pruebas de aceptación

Una vez extraídos los casos de uso y los requisitos del sistema, es posible diseñar un plan de pruebas de aceptación. En este plan de pruebas se definen una serie de condiciones de entrada y la salida esperada para cada una de ellas.

Es de considerar que los requisitos funcionales RF-01, RF-02, RF-03 y RF-04 serán probados en cada una de las pruebas, ya que son requisitos referentes a la tecnología utilizada. No se incluirán en la lista de elementos probados por simplificación pero deben ser tenidos en cuenta.

Pruebas de aceptación			
Id	**Requisitos probados**	**Entrada**	**Salida**
PA-01	RF-05, RF-06, RF-09, RF-10, RF-11, RF-17	Compartir un nuevo álbum. El propietario debe iniciar el proceso de compartición de un álbum en el que, al final del mismo, se notificará a los co-propietarios de la necesidad de su intervención.	Álbum en proceso de compartición con los co-propietarios del mismo notificados de que se requiere su intervención para completar el proceso.
PA-02	RF-06, RF-07, RF-08, RF-09, RF-17	Votación de los co-propietarios. Los co-propietarios del álbum deben acceder a la votación de la política de control de acceso que un propietario ha iniciado.	Álbum con política de control de acceso definida y expuesto en la lista de álbumes a los que es posible acceder.
PA-03	RF-12, RF-13, RF-14, RF-16, RF-17	Acceso positivo a un álbum. Un usuario debe acceder a un álbum de fotos cuya política de control de acceso sea cumplida por éste. Para ello se chequeará la credencial que posee.	El usuario debe poder visualizar el álbum.
PA-04	RF-12, RF-13, RF-14, RF-15, RF-17	Acceso negativo a un álbum. Un usuario debe acceder a un álbum de fotos cuya política de control de acceso no sea cumplida por éste. Para ello se chequeará la credencial que posee.	El usuario no debe poder visualizar el álbum.
PA-05	RF-05, RF-06, RF-07, RF-08, RF-09, RF-10, RF-11, RF-17	Política de control de acceso. Se debe realizar todo el proceso de compartición del álbum escogiendo en cada caso la primera preferencia para cada ámbito.	La política de acceso final debe ser la primera de las preferencias en cada ámbito.
PA-06	RF-05, RF-06, RF-07, RF-08, RF-09, RF-10, RF-11, RF-17	Política de control de acceso. Se debe realizar todo el proceso de compartición del álbum con cuatro participantes, escogiendo dos de ellos la primera preferencia y los otros dos la segunda preferencia para cada ámbito.	La política de acceso final debe ser la segunda de las preferencias en cada ámbito.

Tabla 7. Pruebas de aceptación

Capítulo 4

Diseño detallado

4.1 Diseño de software

En esta sección se realiza una descripción en detalle de los componentes resultantes del análisis. Tras esta descripción será posible comenzar a implementar el sistema ya que quedará bien definido.

Como se decidió en el capítulo anterior, el componente servidor debe ser implementado bajo la tecnología Java en un servidor Apache Tomcat y el componente cliente, en su gran mayoría, bajo la tecnología HTML y JavaScript. Es por esto por lo que el diseño estará orientado a estas tecnologías webs, haciendo uso de Servlets en el caso del servidor y de páginas web en el caso del cliente.

De este modo, se parte del diagrama de componentes definitivo obtenido tras el diseño, representado en la Figura 20, y se detallará en las siguientes subsecciones cada uno de ellos. No se mostrarán las variables de control o métodos de asignación de cada clase. El componente *Interfaz de usuario* tampoco será detallado ya que únicamente consta de las páginas web utilizadas. Lo mismo ocurre con *Datos Facebook*, ya que es un componente externo al sistema y no se desarrollará como tal; únicamente se realizarán consultas para obtener sus datos.

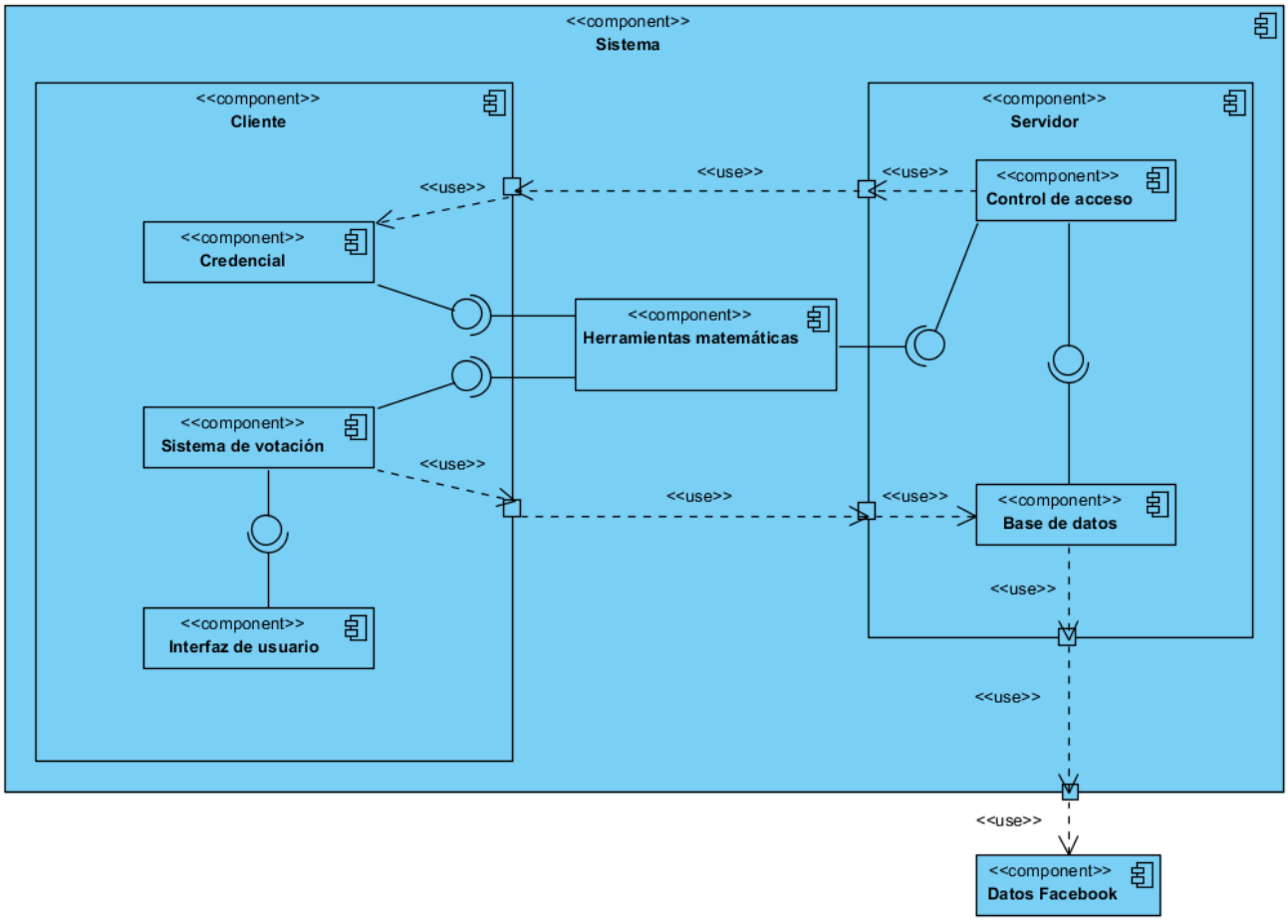

Figura 20. Diagrama de componentes definitivo

4.1.1 Componente *Credencial*

La función de este componente es generar resultados parciales a partir de una credencial anónima, que deberán ser enviados al componente de control de acceso. Estos resultados deberán ser usados para comprobar si el usuario posee permiso para acceder a un álbum de forma que no se revelen nunca los datos reales obtenidos de la credencial (la edad, el grado de discapacidad y la nacionalidad).

Los resultados que se obtengan en este componente servirán de entrada para el componente *Control de acceso*. Por tanto son dos sistemas complementarios donde una parte realiza las pruebas y la otra las verifica. En la Figura 21 se expone el diagrama de clases realizado para el componente Credencial.

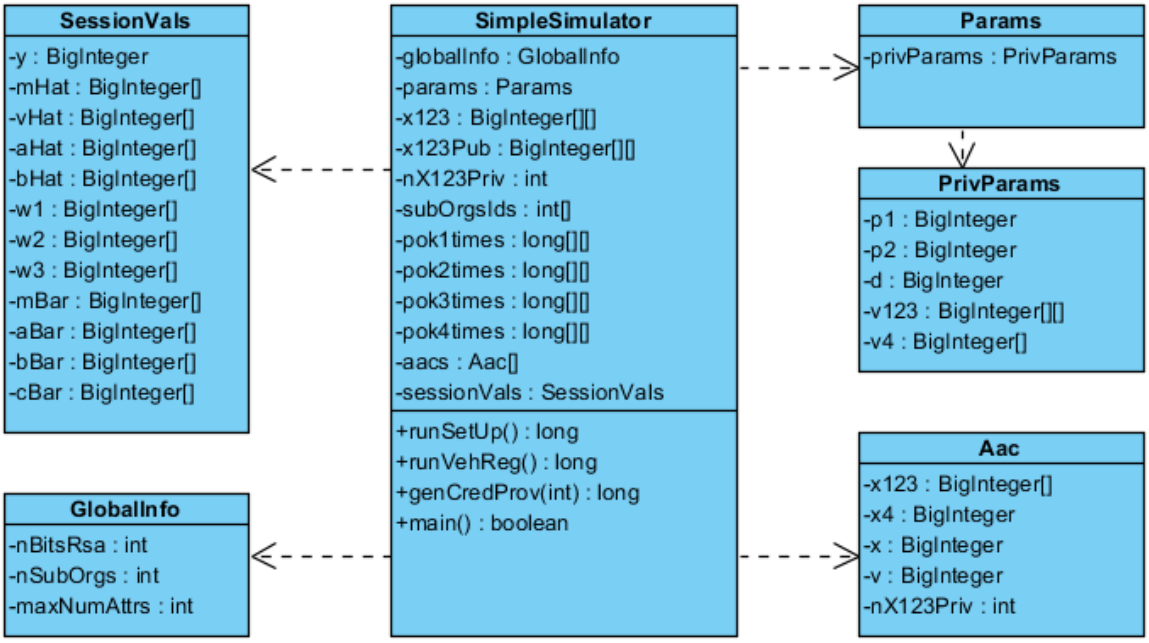

Figura 21. Diagrama de clases, componente Credencial

En él se observan las seis clases que lo componen. *SimpleSimulator* es la principal, y se encarga de obtener los datos de la credencial y realizar sobre ellos una serie de pruebas matemáticas donde se obtendrán los resultados parciales ya mencionados. El resto de clases sirven como estructura básica de datos sobre las que se construyen clases como la credencial (*Aac*) y los parámetros de generación de las pruebas (*SessionVals, GlobalInfo, Params* y *PrivParams*). Las funciones más destacadas son la de generación de los parámetros de sesión (*runSetUp()*) y la que genera los valores que posteriormente se comprobarán en la parte servidora (*genCredProv()*).

4.1.2 Componente *Sistema de votación*

La funcionalidad principal de este componente es la de poner a disposición del usuario un sistema de votación de la política de control de acceso de un álbum. Para ello se ha elaborado la Figura 22, que se corresponde con el diagrama de clases del sistema de votación.

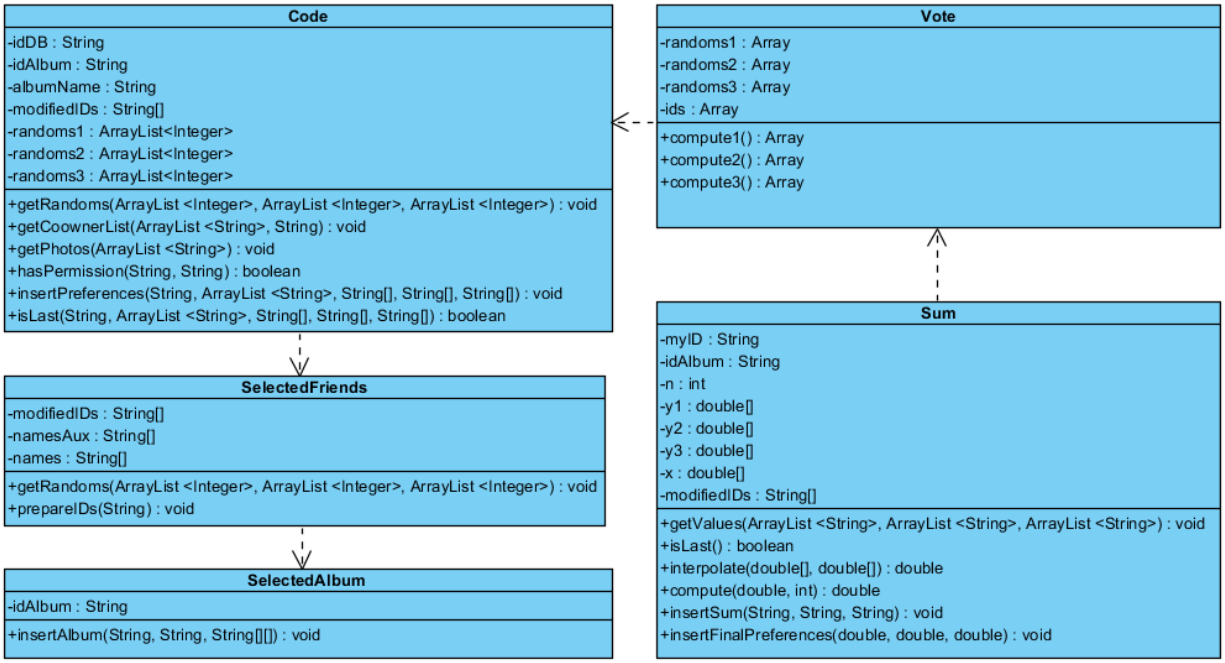

Figura 22. Diagrama de clases, componente Sistema de votación

El componente *SelectedAlbum* se usa después de elegir el álbum sobre el que se va a realizar la votación. Tras esto, se escogen los amigos de Facebook con los que se va a participar, representándolo en la clase *SelectedFriends*. La clase *Code* se encarga de generar los valores aleatorios para aplicar el algoritmo JRSS [28] a la votación, con el fin de preservar el anonimato de la votación, y de preparar los identificadores y valores utilizados. La votación de la política de control de acceso se realiza en la propia página web, por lo tanto la clase *Vote* representa esta página y la tecnología utilizada en ella será JavaScript. Finalmente, cuando todos los co-propietarios han votado, se realiza la funcionalidad de la clase *Sum*¸ la cual se encarga de realizar una interpolación de Lagrange sobre los valores obtenidos en el paso anterior, computando de esta manera la política final.

Se describirán a continuación las funciones más destacables. La de obtención de números aleatorios, *getRandoms()*, genera números aleatorios seguros para la aplicación del algoritmo. La función *prepareIDs()* se encarga de preparar los identificadores que se van a usar, obteniendo los tres últimos dígitos del ID real de Facebook de todos los co-propietarios. Las funciones *compute()* de la clase *Vote* se encargan de aplicar el algoritmo JRSS a los valores, y recoge valores que posteriormente se almacenarán en la clase *Sum* mediante las funciones *insert()*. Finalmente, si el usuario que ha votado es el último, se disparan las funciones *interpolate()* y *compute()* de la clase *Sum*, de forma que se produce la interpolación de Lagrange sobre los valores obtenidos para cada preferencia y se computa el valor final de la misma.

4.1.3 Componente *Herramientas matemáticas*

El componente *Herramientas matemáticas* se compone de una única clase que utilizarán los demás componentes como base matemática para sus cálculos. La Figura 23 representa el diagrama de clases correspondiente.

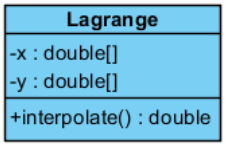

Figura 23. Diagrama de clases, componente Herramientas matemáticas

En este diagrama se puede apreciar la clase *Lagrange*, que se encarga de poner a disposición de los demás componentes la librería matemática asociada para realizar el cálculo de la interpolación de Lagrange sobre un punto. Se compone de dos variables, *x* e *y*, las cuales representan los valores que toma el eje de coordenadas para cierta función. El método *interpolate()* hace efectiva la llamada a la librería y devuelve el valor calculado.

4.1.4 Componente *Control de acceso*

El componente *Control de acceso* tiene como función principal realizar una comprobación sobre una credencial anónima, de forma que se permita o deniegue al usuario el acceso a visualizar el álbum que ha seleccionado en base a si cumple la política de control de acceso o no. La Figura 24 representa el diagrama de clases realizado para este componente.

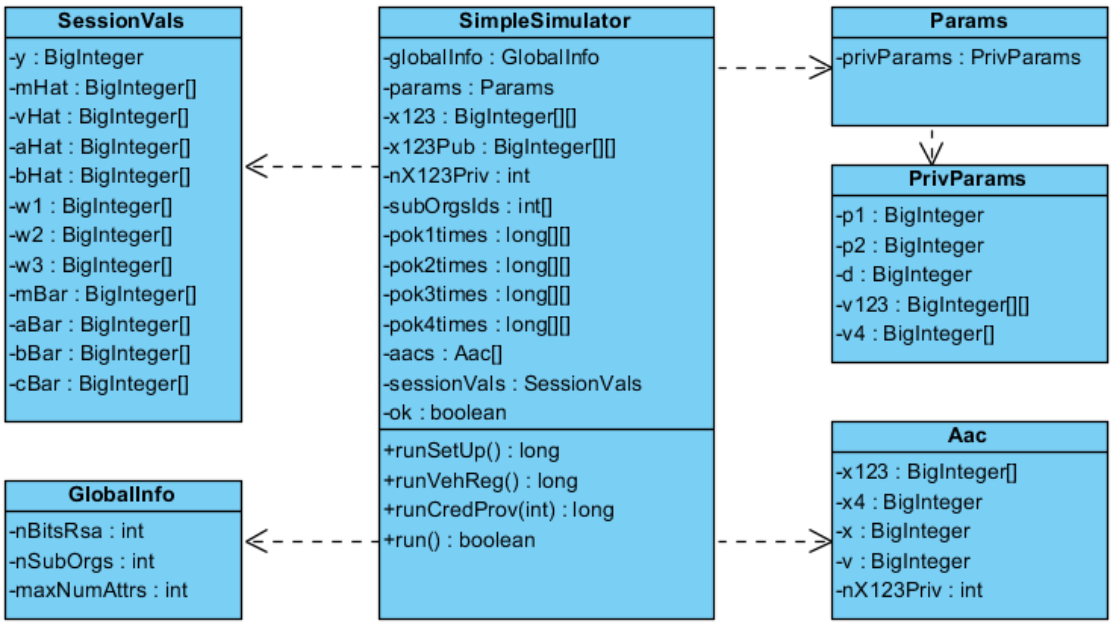

Figura 24. Diagrama de clases, componente Control de acceso

Como se puede apreciar, la estructura básica es la misma que la del componente *Credencial*, ya que, como se mencionó, son sistemas complementarios. Esta parte trata de verificar los datos obtenidos tras las pruebas locales con la credencial. Al igual que en el componente *Credencial*, las clases *SessionVals*, *GlobalInfo*, *Params*, *PrivParams* y *Aac* sirven como estructura básica de datos de la sesión y como parámetros de las pruebas a realizar. La clase *SimpleSimulator* se encarga de poner en marcha toda la funcionalidad, destacando las funciones *runSetUp()*, que inicializa los parámetros de sesión de igual forma que en el paso anterior, y la función *runCredProv()*, que realiza las comprobaciones sobre los datos obtenidos. La función *run()* es la función principal y devuelve un booleano, que será "true" si la comprobación es correcta y por tanto el usuario tiene permiso para acceder, o "false" si de lo contrario no posee permiso para acceder a visualizar el álbum de fotos.

4.1.5 Componente *Base de datos*

Este componente representa la base de datos que se utilizará en la aplicación para almacenar los valores relevantes. La Figura 25 describe el diagrama de clases de la base de datos.

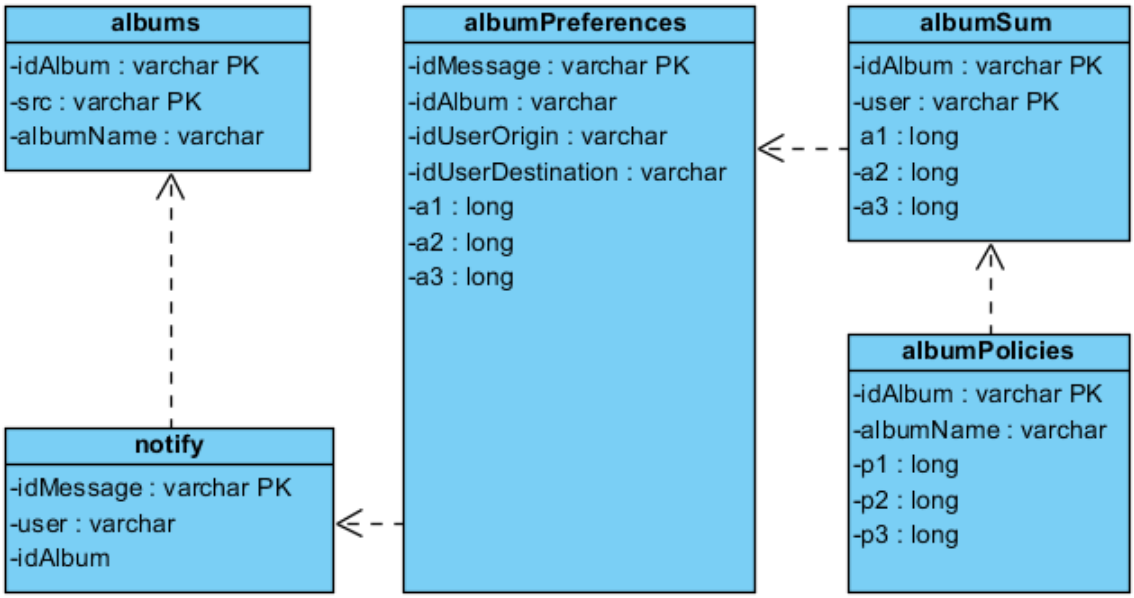

Figura 25. Diagrama de clases, componente Base de datos

En este caso, cada clase representa una tabla y cada atributo las columnas de la tabla. Así pues, se describirán a continuación cada una de ellas.

- *albums*: esta tabla almacena las direcciones reales de cada fotografía en Facebook, de forma que se pueda mostrar al usuario el álbum en cuestión. En ella se almacena el identificador real del álbum, su nombre real y la dirección web de la fuente. *Nota: Es remarcable que el uso que hace Facebook de este sistema de fotografías resulta una violación de la privacidad de los usuarios, ya que introduciendo esta dirección fuente en un navegador web es posible visualizar la imagen en cuestión sin ningún tipo de filtro por parte de Facebook.*

- *notify*: esta tabla se utiliza para que el sistema pueda llevar un control sobre a quién se le ha notificado de que se requiere su intervención en la votación. Para ello, se almacena el identificador de usuario real, el identificador del álbum sobre el que se realiza la votación y un número aleatorio, que será un código que el usuario deberá introducir en la aplicación, proporcionando de esta forma una pasarela de seguridad para posibles suplantaciones de identidad.

- *albumPreferences*: se utiliza para almacenar los valores necesarios para el algoritmo JRSS. Estos valores son los identificadores de los usuarios, los valores que cada uno ha calculado (excepto los suyos propios, que deberán almacenarlos los propios usuarios, preservando así el anonimato del voto), el identificador del álbum en cuestión y un número aleatorio de control.

- *albumSum*: aquí se almacenan los datos sumados localmente por la máquina cliente de cada usuario, necesario para la aplicación del algoritmo JRSS. Los datos en cuestión son el identificador del álbum, el identificador del usuario que ha realizado la suma y el valor calculado para cada preferencia.

- *albumPolicies*: finalmente, esta tabla se encarga de almacenar la política de control de acceso final computada tras la realización de la interpolación de Lagrange para cerrar el círculo del algoritmo JRSS. Se almacenan el nombre del álbum, su identificador real y la política elegida para cada preferencia.

4.2 Diagramas de secuencia

Tras realizar el diseño software del sistema, se procede a incluir los diagramas de secuencia. Estos diagramas reflejan las interacciones entre el usuario y el sistema, así como sus clases. Esta sección toma de base las interacciones definidas en la sección 3.6.

No se mostrarán los flujos alternativos, ya que la secuencia principal debe ser la que se produzca en la gran mayoría de los casos

4.2.1 Compartir nuevo álbum (CU-01)

La Figura 26 muestra el diagrama de secuencia para el caso de uso CU-01.

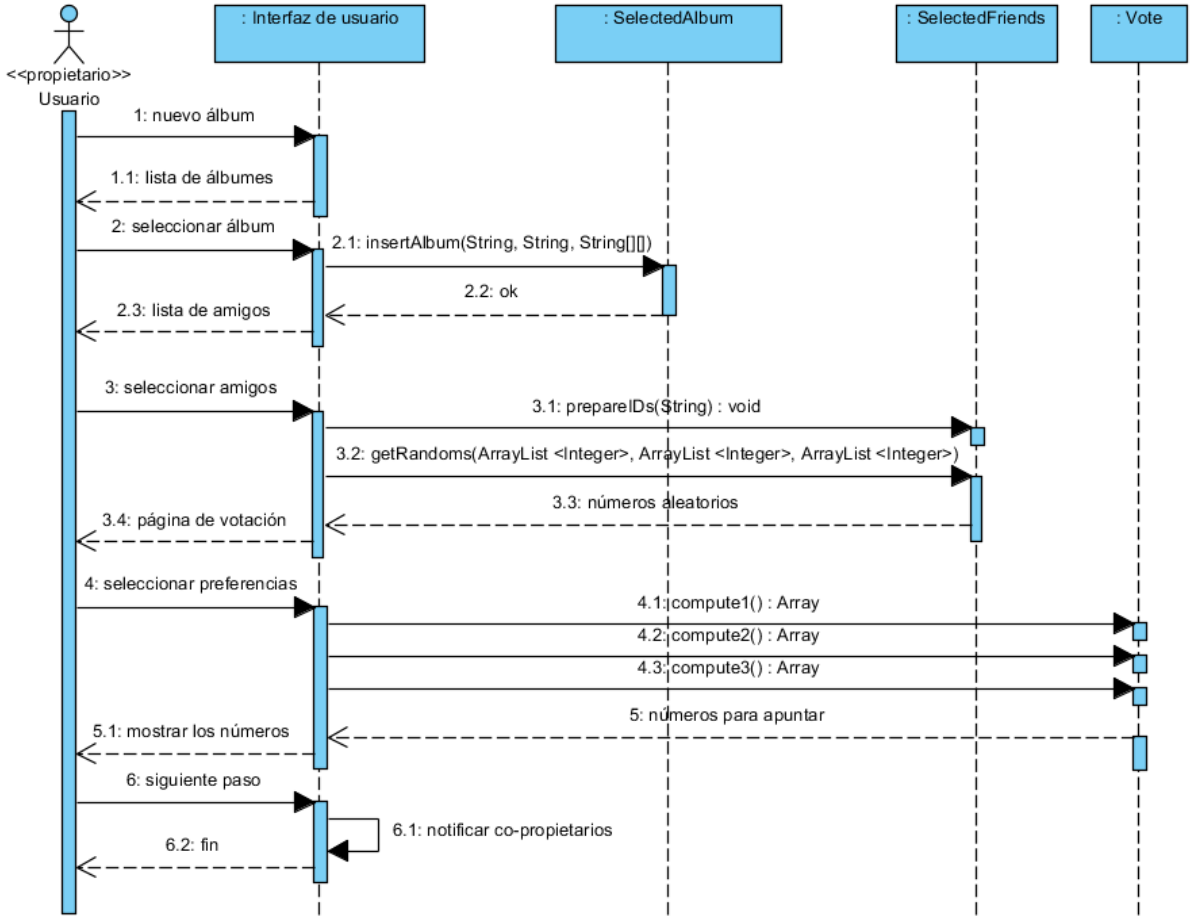

Figura 26. Diagrama de secuencia de Compartir nuevo álbum (CU-01)

Este diagrama describe el proceso de compartición de un nuevo álbum por parte del propietario. En primer lugar se debe seleccionar cuál se desea compartir, haciendo uso de la interfaz. Seguidamente el sistema procede a insertar el álbum en la base de datos y a

mostrar al usuario la lista de amigos con los que puede compartirlo, que serán los co-propietarios del álbum. Una vez seleccionados los deseados, se modifican sus identificadores para poder hacer uso del algoritmo, se generan números aleatorios para construir el polinomio necesario y se traslada al usuario a la página de votación. Éste hace su elección para cada una de las preferencias, el sistema calcula en la máquina cliente los valores necesarios y devuelve al usuario los números que deberá apuntar para preservar su anonimato. Por último, el usuario notifica de forma automática a los co-propietarios del álbum que se requiere su intervención en el sistema.

4.2.2 Introducir preferencias (CU-02)

La Figura 27 muestra el diagrama de secuencia para el caso de uso CU-02.

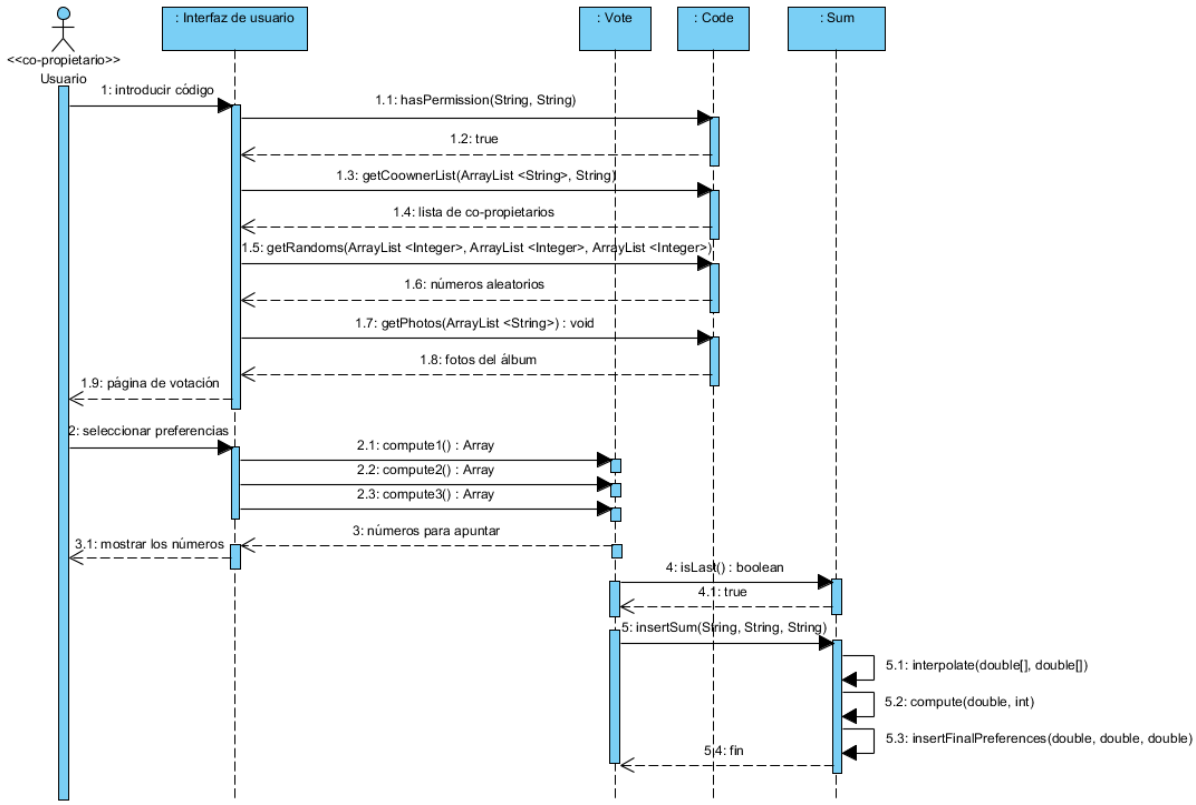

Figura 27. Diagrama de secuencia de Introducir preferencias (CU-02)

Este diagrama de secuencia describe el proceso que cada uno de los co-propietarios deberá seguir para hacer efectiva su votación en el álbum a compartir. En primer lugar el usuario debe introducir el código recibido, el cual chequea el sistema para comprobar que tiene permiso a acceder. En caso afirmativo, el sistema recupera la lista de co-propietarios, genera los números aleatorios y recoge el álbum para mostrar al usuario una previsualización del mismo. Seguidamente se le redirige a la página de votación, donde selecciona su opción para cada una de las preferencias. Cuando éste acaba, se le muestran los valores que debe apuntar y el sistema comprueba si ha sido el último en seleccionarlas para realizar el cómputo final, donde se inserta la suma de los valores del algoritmo, se realiza una interpolación con todas las sumas y se computa la preferencia. Finalmente se inserta en la base de datos la preferencia final calculada para el álbum.

4.2.3 Visualizar álbum (CU-03)

La Figura 28 muestra el diagrama de secuencia para el caso de uso CU-03.

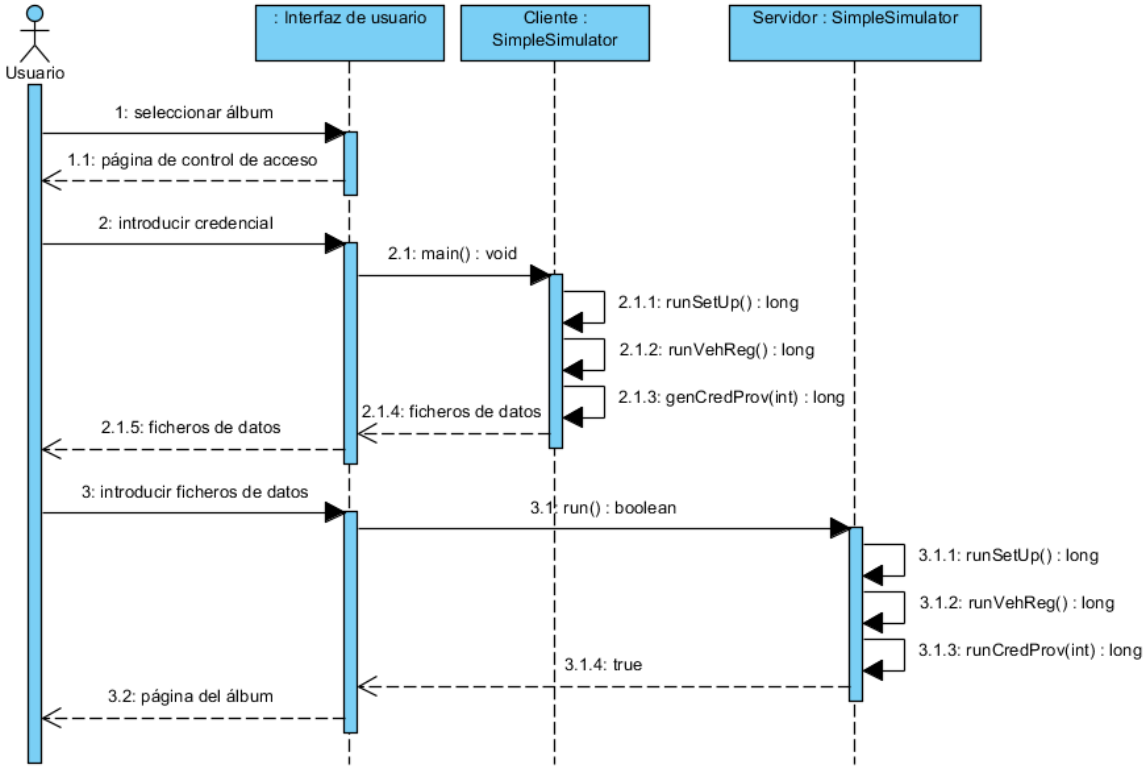

Figura 28. Diagrama de secuencia de Visualizar álbum (CU-03)

Este diagrama representa la acción de un usuario que posee una credencial anónima y desea acceder a visualizar un álbum previamente compartido en el sistema y la respuesta positiva del mismo. Para ello, selecciona el álbum que desea y la página le impone el control de acceso. El usuario arranca en su máquina local la aplicación de preparación de los datos de la credencial, para preservar el anonimato, y, tras realizar ésta los cálculos sobre los datos obtenidos, devuelve varios ficheros de datos binarios al usuario. Seguidamente estos ficheros debe introducirlos en la página correspondiente, haciendo una llamada ahora a la parte servidora de la aplicación de chequeo de credenciales que, tras realizar el resto de los cálculos, permite (o no) el acceso al álbum.

Capítulo 5

Implementación y pruebas

5.1 Aspectos de la implementación

En esta sección se comentarán los aspectos más relevantes de la implementación. Se destaca la conexión que se realiza con Facebook para obtener los datos así como aspectos relativos a la seguridad de los datos y decisiones de implementación.

5.1.1 Conexión con Facebook

Como se estableció en el capítulo 3 de este documento, se ha establecido el SDK de JavaScript como medio de consulta de datos de la red social. Para poder acceder a ellos, en primer lugar se debe dar de alta una aplicación en Facebook. Seguidamente, para obtener algún dato, ésta debe comprobar que hay una sesión iniciada por el usuario. La primera vez que éste accede, se le solicitan permisos específicos en función de los datos que se pretenden extraer. De esta manera, la Figura 29 representa el proceso de autenticación por parte del usuario y la autorización de la aplicación.

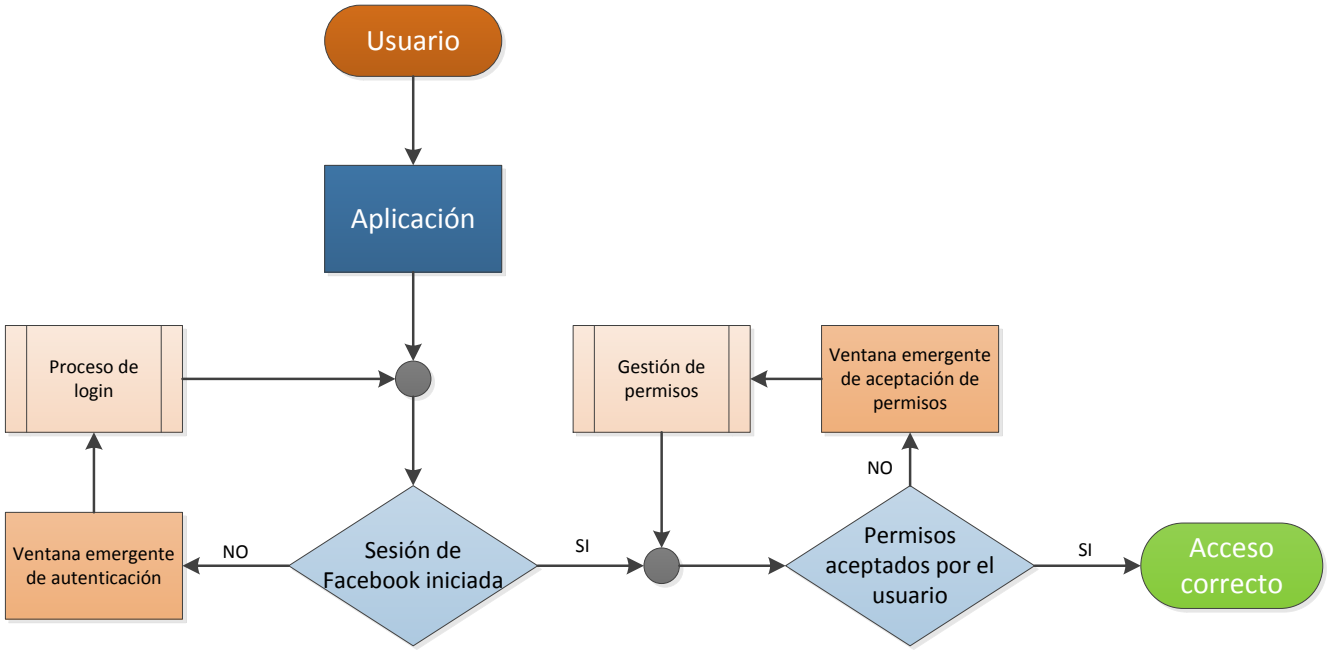

Figura 29. Proceso de obtención de datos

Para que la aplicación se mantenga en constante conexión con Facebook, se requiere autenticar la aplicación ante la red social en todo momento. Para ello se utiliza la función que aparece en la Figura 30, la cual proporciona el identificador *appId* a la red social para verificar su autenticidad.

```
window.fbAsyncInit = function() {
  FB.init({
    appId      : '533027363416918', // App ID from the App Dashboard
    channelUrl : 'http://young-taiga-6653.herokuapp.com/channel.html', // Channel File for x-domain communication
    status     : true, // check login status
    cookie     : true, // enable cookies to allow the server to access the session
    xfbml      : true  // parse XFBML
  });
```

Figura 30. Autenticación de la aplicación

Se requiere también cargar las librerías de funcionalidades de Facebook, para lo cual se utiliza la función de la Figura 31. En el atributo *src* de la variable *js* está definida la ruta de dicha librería.

```
(function(d){
   var js, id = 'facebook-jssdk', ref = d.getElementsByTagName('script')[0];
   if (d.getElementById(id)) {return;}
   js = d.createElement('script'); js.id = id; js.async = true;
   js.src = "//connect.facebook.net/en_US/all.js";
   ref.parentNode.insertBefore(js, ref);
 }(document));
```

Figura 31. Carga de librerías

Como último paso para que la aplicación conecte correctamente con la red social, se requiere consultar el estado de la sesión del usuario. Para ello se utiliza la función de consulta reflejada en la Figura 32, donde se chequea el atributo *status* de la respuesta que da el servidor. Si su valor es "connected" significa que el usuario está conectado y ha autorizado ya a la aplicación. Si el resultado es "not_authorized" quiere decir que el usuario se encuentra conectado pero aún no ha autorizado a la aplicación. Finalmente, si el resultado es "not_connected" significa que el usuario no posee una sesión abierta de Facebook y que por lo tanto no se encuentra conectado.

```
FB.getLoginStatus(function(response) {
  if (response.status === 'connected') {
      document.getElementById("log").value = "connected";
      uid = response.authResponse.userID;
      perm = true;
  } else if (response.status === 'not_authorized') {
      // not_authorized
      document.getElementById("log").value = "not_authorized";
      alert("You have not auothorized this app yet");
      login();
  } else {
      // not_logged_in
      document.getElementById("log").value = "not_connected";
      alert("You have not logged into Facebook");
      login();
  }
});
```

Figura 32. Estado de conexión

En cualquier caso, la aplicación ofrece un botón de autenticación donde se establecen además los permisos adicionales que necesitará la aplicación; obtener las fotos del usuario en este caso. (Figura 33)

```
<fb:login-button scope="user_user_photos">
    Login
</fb:login-button>
```

Figura 33. Botón de autenticación

5.1.2 Aspectos de seguridad

Actualmente la seguridad de la información digital es primordial para cualquier usuario. Por ello, los aspectos de seguridad relacionados con esta aplicación han sido considerados de forma que se dificulten los posibles ataques que se puedan producir. En resumen, se han adoptado las siguientes medidas de seguridad.

- Conexión SSL: El primer aspecto que es necesario cubrir en cualquier aplicación web es integrar el protocolo SSL [29] a la comunicación que se establece entre el cliente y el servidor. Para ello, se ha instalado el certificado firmado por una autoridad (en este caso autofirmado) en el servidor Apache Tomcat y se ha configurado el servidor para que haga uso del protocolo SSL. Así pues, se establece una conexión cifrada entre cliente y servidor que dificulta los ataques de hombre en el medio. [30]

- Conexión segura a la base de datos: Con la pretensión de que los datos son accedidos de forma segura, se ha configurado en el servidor MySQL un usuario con permisos de acceso a la base de datos de la aplicación y se le ha proporcionado una contraseña. Un aspecto que se consideró fue el cifrado de la base de datos, pero se rechazó ya que, para álbumes muy grandes, las consultas y las inserciones se demorarían considerablemente.

- Utilización del algoritmo JRSS: Este algoritmo es utilizado en el proceso de votación para hacerla efectiva de un modo anónimo. Su nombre viene del inglés, "Joint Random Secret Sharing", y está pensado para compartir una información secreta entre varios usuarios mediante su ocultación por métodos que aprovechan las ventajas que ofrece la aritmética modular [28]. Así pues, las preferencias que escoja cada usuario no viajarán a la máquina servidora y, por tanto, no habrá forma de averiguar su elección.

- Utilización de credenciales anónimas: Se ha simulado la utilización de credenciales anónimas mediante la generación de éstas de forma local y la verificación de la política de control de acceso para una en concreto. Este es un aspecto importante para la seguridad de los usuarios que tratan de acceder a visualizar un álbum, ya que con la utilización del sistema de credenciales anónimas se preservarán los datos en la máquina del usuario mediante la realización de pruebas locales. De esta forma, los datos de carácter privado de la credencial se mantendrán seguros sin que ninguno viaje a través de Internet.

- Comprobación del estado de conexión: Existe la posibilidad de que, por un motivo u otro, la sesión que el usuario tiene abierta en Facebook se cierre mientras se está utilizando la aplicación. Si no se comprobase en cada una de las páginas de la misma el estado de la conexión, podrían mostrarse datos privados sin que se tuvieran los permisos adecuados para ello. Así pues, cada una de las páginas realiza una consulta a la red social para cerciorarse de que la sesión sigue abierta.

- Generación segura de números aleatorios: En este sistema es muy frecuente que sea necesario generar números aleatorios. Uno de los pilares fundamentales del algoritmo JRSS y de los algoritmos de comprobación de las credenciales es hacer uso de números al azar. Existen librerías básicas de generación [31], pero se basan en patrones inseguros [32]; es por esto que se utiliza la clase *SecureRandom* de Java para la generación de estos números [33].

5.2 Resultados de las pruebas de aceptación

La Tabla 8 muestra los resultados de las pruebas de aceptación definidas en la sección 3.8. Tal y como se podrá comprobar, se han completado todas las pruebas con éxito, lo que garantiza una correcta implementación del sistema.

Resultados de las pruebas de aceptación		
Id	**Requisitos probados**	**Resultado**
PA-01	RF-05, RF-06, RF-09, RF-10, RF-11, RF-17	Superada
PA-02	RF-06, RF-07, RF-08, RF-09, RF-17	Superada
PA-03	RF-12, RF-13, RF-14, RF-16, RF-17	Superada
PA-04	RF-12, RF-13, RF-14, RF-15, RF-17	Superada
PA-05	RF-05, RF-06, RF-07, RF-08, RF-09, RF-10, RF-11, RF-17	Superada
PA-06	RF-05, RF-06, RF-07, RF-08, RF-09, RF-10, RF-11, RF-17	Superada

Tabla 8. Resultados de las pruebas de aceptación

Capítulo 6

Conclusiones y líneas futuras

6.1 Conclusiones sobre el trabajo

En esta sección se exponen las conclusiones extraídas tras la finalización del trabajo de fin de grado. Se analizarán a continuación los resultados principales, las dificultades encontradas y se comentarán las conclusiones personales.

6.1.1 Resultados obtenidos

Se ha desarrollado con éxito una herramienta que permite a múltiples usuarios crear conjuntamente una política de control de acceso común para un álbum de fotos. Esto ha solventado el gran problema que supone para los co-propietarios no disponer de herramientas para gestionar la co-propiedad de los contenidos.

Otro de los aspectos desarrollados ha sido el del anonimato en el sistema de votación para una política común. Gracias a técnicas matemáticas ha sido posible ocultar las preferencias que cada usuario ha escogido en el proceso de la votación. Por lo tanto, el objetivo número 1, "crear un sistema de votación conjunta y anónima que permita a propietarios y co-propietarios gestionar el acceso a sus contenidos" ha sido satisfecho.

Por otra parte, el objetivo número 2, "realizar un mecanismo de control de acceso a los álbumes del sistema basado en la comprobación de una credencial de forma anónima", también ha sido satisfecho.

En definitiva, el desarrollo de este de fin de grado proporciona un sistema para que propietarios y co-propietarios gestionen conjuntamente la privacidad de sus álbumes de fotos, a la vez que se consigue que el acceso a dichos álbumes sea anónimo. Esto contribuye positivamente a la sociedad ya que mejora los medios de compartición existentes en las redes sociales. Bien es cierto que supone cierto esfuerzo económico porque requiere modificar elementos actuales de las redes sociales e introducir nuevos elementos como la credencial.

Finalmente, cabe mencionar que la implementación realizada en este proyecto forma parte del desarrollo de un artículo de investigación.

6.1.2 Dificultades del trabajo de fin de grado

A lo largo de todo el trabajo de fin de grado, se han afrontado múltiples dificultades.

En primer lugar, surgió una dificultad en la etapa del análisis, donde hubo que definir la arquitectura del sistema, ya que hubo que pensar cómo compaginar el sistema de votación con el anonimato y con el sistema de acceso por credenciales, lo que llevó mucho más tiempo de lo esperado, junto con decisiones erróneas.

En segundo lugar, en la etapa de diseño se sufrió otro retraso importante, derivado de la necesidad de utilizar una arquitectura cliente-servidor, donde se requerían datos comunes a ambos lados del sistema. Esto, junto con la modificación un sistema de credenciales centralizado para hacerlo distribuido, repercutió negativamente en la planificación inicial del trabajo de fin de grado.

Finalmente, la dificultad más acusada de todas fue en la etapa de implementación. Existieron innumerables complejidades a lo largo de toda esta etapa, pero las más interesantes fueron las que se comentan a continuación. La primera de ellas fue obtener datos de Facebook y pasarlos al servidor y obtener datos del servidor y pasárselos al cliente, ya que en muchos de los casos hubo que procesar los datos previamente para darles un formato que pudiera recogerse con facilidad al otro lado. Muchas de las incoherencias que se obtenían al realizar pequeñas pruebas eran debidos a que, a veces, el servidor de Facebook no respondía correctamente, pero se pensó que eran problemas del sistema, lo que dio lugar a mucho tiempo de revisión de código que en realidad era correcto. Por último, otro de los problemas fue traducir las operaciones matemáticas necesarias del papel al código, y hacerlo además de forma que no se pudiera desbordar el rango máximo de los números, lo que dio lugar a múltiples conversiones de formatos.

6.1.3 Conclusiones personales

A pesar de que el trabajo de fin de grado haya sido un trabajo que requiere mucha dedicación y a la vez en el que han surgido múltiples dificultades a las que hacer frente, ha aportado una experiencia muy valiosa. Se puede decir que, a lo largo de toda la carrera, las asignaturas contribuyen con pequeñas porciones de conocimiento “aislado” y que el trabajo de fin de grado las agrupa a todas ellas para proponer una solución a un problema real.

Por otra parte, el trabajo de fin de grado ha supuesto un gran reto investigador, ya que se han tenido que realizar diversos estudios sobre el estado de las redes sociales, sobre los algoritmos matemáticos utilizados y sobre el estado de la investigación en este campo. Como consecuencia, haber desarrollado un sistema novedoso y que va un paso más allá de todo lo existente, supone una gran satisfacción personal ya que, además, contribuye positivamente en la sociedad.

6.2 Líneas futuras

En esta sección se enumeran posibles ampliaciones del sistema actual que se han identificado a lo largo de todo el trabajo de fin de grado.

6.2.1 Extensibilidad a cualquier tipo de contenido

La aplicación desarrollada centra su funcionalidad en decidir la política de control de acceso para álbumes de fotos. Teniendo en cuenta que las políticas son las mismas para cualquier tipo de contenido, ya sea una foto individual, un vídeo, un enlace o cualquier tipo de contenido que implique a varios usuarios, este sistema sería aplicable a cualquier contenido.

6.2.2 Implementación del acceso anónimo completo

Actualmente, el sistema de generación, comprobación y verificación de credenciales es un simulador que las genera, comprueba y verifica para una política concreta. Por ello, como trabajo futuro se plantea la completa implementación del sistema de acceso por credenciales anónimas.

6.2.3 Integración de Tor

Tor, del inglés *The Onion Router* [34], es un proyecto de software libre sobre enrutamiento que trata de desarrollar una red distribuida construida sobre Internet cuyo objetivo es no revelar la dirección IP de los mensajes intercambiados entre los usuarios, manteniendo de forma adicional su integridad y su confidencialidad. Si un usuario accede de forma continua a un álbum de fotos, aunque no se pueda saber quién es, se puede saber que esa persona ha accedido varias veces ya que la dirección IP de los mensajes de acceso sería la misma. De esta forma, si se añadiera este sistema a la aplicación, se conseguiría anonimato a nivel de red, proporcionando así un sistema completamente anónimo.

6.2.4 Adición de un sistema de cookies

Las cookies son información que almacenan los sitios web en las máquinas de sus usuarios. Una posible mejora de la aplicación consiste en utilizar cookies para almacenar los valores que se obtienen en los procesos intermedios de forma que el usuario no tuviera que introducirlos más adelante. De esta forma mejoraría la usabilidad de la aplicación ya que el usuario no debería anotar los valores obtenidos en el proceso de votación.

6.2.5 Preferencias flexibles

El escenario sobre el que se ha desarrollado la aplicación ha hecho que las preferencias sobre las que los usuarios deben votar la política de control de acceso sean la edad, el grado de discapacidad y la nacionalidad. Atendiendo a la flexibilidad del sistema propuesto, como futuro trabajo se plantea la creación de nuevas preferencias. El sistema podría ser ampliado desplegando una lista de preferencias para que el propietario escoja las que desee incluir en las políticas de control de acceso creadas.

6.2.6 Implementación en dispositivos móviles

Una posible ampliación del sistema consiste en, aprovechando la API que Facebook ofrece tanto para iOS [15] como para Android [14], implementar el sistema de votación en plataformas. De esta forma, se aumentaría la portabilidad de la aplicación.

Referencias

[1] Sorav Jain. (2012, Octubre) Social Media Today. [Online]. http://socialmediatoday.com/node/195917

[2] Facebook. (2013) Facebook - Muro. [Online]. https://www.facebook.com/help/search/?query=muro

[3] Facebook. (2012, Diciembre) Facebook. [Online]. https://www.facebook.com/about/privacy/

[4] Jefatura del Estado. (2000, Enero) Ley Orgánica 15/1999. [Online]. http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf

[5] A. Lysyanskaya F. Baldimtsi, "Anonymous Credentials Light," *IACR Cryptology ePrint Archive*, 2012.

[6] Bebo. (2009, Marzo) Privacy Policy. [Online]. http://www.bebo.com/Privacy2.jsp

[7] LinkedIn. Política de Privacidad. [Online]. http://www.linkedin.com/static?key=privacy_policy&trk=hb_ft_priv

[8] Twitter. (2012, Mayo) Política de Protección de Datos de Twitter. [Online]. https://twitter.com/privacy

[9] Myspace. (2012, Octubre) Myspace. [Online]. http://www.myspace.com/Help/Privacy

[10] Mohamed Shehab, Joshua Wede Anna C. Squicciarini, "Privacy policies for shared content in social network sites," *The VLDB Journal*, Junio 2010.

[11] Domenico Corapi, Srdjan Marinovic, Morris Sloman Ryan Wishart, "Collaborative Privacy Policy Authoring in a Social Networking Context," *Policies for Distributed Systems and Networks (POLICY), 2010 IEEE International Symposium on*, Julio 2010.

[12] Heng Xu, Xiaolong (Luke) Zhang Anna C. Squicciarini, "CoPE: Enabling Collaborative Privacy Management in Online Social Networks," *Journal of the American Society for Information Science and Technology*, Marzo 2011.

[13] Gail-Joon Ahn, Jan Jorgensen Hongxin Hu, "Multiparty Access Control for Online

Social Networks: Model and Mechanisms," *IEEE Transactions on Knowledge and Data Engineering*, Abril 2012.

[14] Facebook. (2013, Julio) Facebook SDK for Android. [Online]. https://developers.facebook.com/android/

[15] Facebook. (2013, Agosto) Facebook SDK for iOS. [Online]. https://developers.facebook.com/ios/

[16] Facebook. (2013, Agosto) Facebook for Web Developers. [Online]. https://developers.facebook.com/docs/web/

[17] Reva Friedman-Nimz, Judith Lacey, Debra Denson Brenna O'Brien, "From Bits and Bytes to C++ and Web Sites: What Is Computer Talent Made of?," *Gifted Child Today*, 2005.

[18] Oracle. (2013) New to Java Programming Center. [Online]. http://www.oracle.com/technetwork/topics/newtojava/downloads/index.html

[19] Mozilla. (2012, Noviembre) JavaScript | MDN. [Online]. https://developer.mozilla.org/es/docs/JavaScript

[20] PHP. (2013, Agosto) PHP: Hypertext Preprocessor.

[21] Apache. (2013) Commons Math. [Online]. http://commons.apache.org/proper/commons-math/

[22] Apache. (2013) Apache Tomcat. [Online]. http://tomcat.apache.org/

[23] IBM. (2009, Febrero) WebSphere Application Server. [Online]. http://pic.dhe.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/rovr_specs.html

[24] Oracle. (2013) Oracle Database. [Online]. http://www.oracle.com/es/products/database/overview/index.html

[25] Oracle. (2013) MySQL. [Online]. http://www.mysql.com/

[26] Facebook. (2013, Junio) Facebook SDK for JavaScript. [Online]. https://developers.facebook.com/docs/reference/javascript/

[27] Facebook. (2013, Agosto) Facebook SDK for PHP. [Online]. https://developers.facebook.com/docs/reference/php/

[28] Ali Aydın Selçuc Kamer Kaya, "A Verifiable Secret Sharing Scheme Based on the Chinese Remainder Theorem," *9th International Conference on Cryptology in India*, 2008.

[29] P. Karlton, P. Kocher A. Freier. (2011, Agosto) RFC 6101 - The Secure Sockets Layer (SSL) Protocol Version 3.0. [Online]. http://tools.ietf.org/html/rfc6101

[30] Erik Hjelmvik. (2011, Marzo) Network Forensic Analysis of SSL MITM Attacks. [Online]. http://www.netresec.com/?page=Blog&month=2011-03&post=Network-Forensic-Analysis-of-SSL-MITM-Attacks

[31] Oracle. (2011) Random (Java Platform SE 6). [Online]. http://docs.oracle.com/javase/6/docs/api/java/util/Random.html

[32] J. Schiller, S. Crocker. (1994, Diciembre) RFC 1750 - Randomness Recommendations for Security. [Online]. http://www.ietf.org/rfc/rfc1750.txt

[33] Oracle. (2013) SecureRandom (Java Platform SE 7). [Online]. http://docs.oracle.com/javase/7/docs/api/java/security/SecureRandom.html

[34] The Tor Project. (2012, Diciembre) Tor Project: Anonymity Online. [Online]. https://www.torproject.org/

[35] Apple. (2013) Apple - Soporte técnico - Snow Leopard. [Online]. http://www.apple.com/es/support/snowleopard/

[36] The Eclipse Foundation. (2010) Eclipse IDE for Java EE Developers. [Online]. http://www.eclipse.org/downloads/packages/eclipse-ide-java-ee-developers/keplerr

[37] Google. (2013) Navegador Chrome. [Online]. http://www.google.com/intl/es_es/chrome/

[38] Microsoft. (2013) Microsoft Office. [Online]. http://office.microsoft.com/es-es/?CTT=97

[39] Microsoft. (2013) Project 2013. [Online]. http://office.microsoft.com/es-es/project/project-online-software-de-administracion-de-carteras-de-proyectos-en-linea-FX103996174.aspx

[40] Microsoft. (2013) Microsoft Windows. [Online]. http://windows.microsoft.com/es-es/windows/home

[41] Oracle. (2013) MySQL Workbench. [Online]. http://www.mysql.com/products/workbench/

[42] Barebones. (2013) TextWrangler. [Online]. http://www.barebones.com/products/textwrangler/

[43] VisualParadigm. (2013) Visual modeling tool for building enterprise applications. [Online]. http://www.visual-paradigm.com/product/vpuml/features/

[44] Universidad Carlos III de Madrid. Plantilla PFC. [Online]. https://www.uc3m.es/portal/page/portal/administracion_campus_leganes_est_cg/proyecto_fin_carrera/Plantilla_PFC.doc

Glosario

Anonimato: concepto que describe una situación donde un usuario no es identificado por el sistema.

Apache Tomcat: servidor web basado en Java utilizado.

Co-propiedad: concepto que describe una situación con un propietario de un contenido donde se identifican otros usuarios que comparten la propiedad del mismo.

Credencial anónima: fichero digital con información real de una persona física, expedido por una autoridad y utilizado en este trabajo de fin de grado para el acceso anónimo de los usuarios.

HTML: *HyperText Markup Languaje*; lenguaje utilizado para la elaboración de las páginas web.

Java: lenguaje de programación orientado a objetos utilizado.

JavaScript: lenguaje de programación web utilizado.

Script: fragmento de código interpretado en tiempo de ejecución.

SQL: *Structured Query Languaje*; lenguaje utilizado para los scripts de la base de datos.

Tor: *The Onion Router*; proyecto dedicado a proporcionar anonimato a nivel de red.

Anexo 1

Gestión del proyecto

1. Planificación del trabajo

En esta sección se exponen la planificación inicial y el desarrollo real del proyecto así como un estudio de las desviaciones presentadas entre ambos.

1.1 Planificación inicial

Se elaboró una planificación inicial para las diferentes fases del trabajo de fin de grado así como el esfuerzo estimado para cada una de ellas. Se ha tenido en cuenta para la elaboración de esta planificación una jornada de trabajo diaria media de tres horas. El motivo de esta decisión es debido a que se ha compaginado el trabajo de fin de grado con el último curso académico del Grado en Ingeniería Informática.

Esta planificación abarca desde el día 21 de febrero del año 2013 hasta el día 15 de junio del mismo año, lo que suman un total de 115 días de trabajo.

La Tabla 9 muestra en detalle la planificación inicial del trabajo de fin de grado.

Planificación inicial			
Trabajo de fin de grado	**115 días**	**jue 21/02/2013**	**dom 15/06/2013**
Planificación inicial	**3 días**	**jue 21/02/2013**	**sáb 23/02/2013**
Estado del arte	**14 días**	**dom 24/02/2013**	**sáb 09/03/2013**
Análisis de las redes sociales	7 días	dom 24/02/2013	sáb 02/03/2013
Estudio de investigación	7 días	dom 03/03/2013	sáb 09/03/2013
Análisis	**15 días**	**dom 10/03/2013**	**dom 24/03/2013**
Arquitectura del sistema	5 días	dom 10/03/2013	jue 14/03/2013
Estudio tecnológico	2 días	vie 15/03/2013	sáb 16/03/2013
Definición de casos de uso	1 día	dom 17/03/2013	dom 17/03/2013
Definición de requisitos	6 días	lun 18/03/2013	sáb 23/03/2013
Diseño del plan de pruebas	1 día	dom 24/03/2013	dom 24/03/2013
Diseño	**20 días**	**lun 25/03/2013**	**sáb 13/04/2013**
Diseño software	14 días	lun 25/03/2013	dom 07/04/2013
Diagramas de secuencia	6 días	lun 08/04/2013	sáb 13/04/2013
Implementación	**40 días**	**dom 14/04/2013**	**dom 23/05/2013**
Pruebas	**3 días**	**vie 24/05/2013**	**dom 26/05/2013**
Documentación	**20 días**	**lun 27/05/2013**	**sáb 15/06/2013**

Tabla 9. Planificación inicial detallada

La Figura 34 muestra el diagrama de Gantt para la planificación inicial del trabajo de fin de grado.

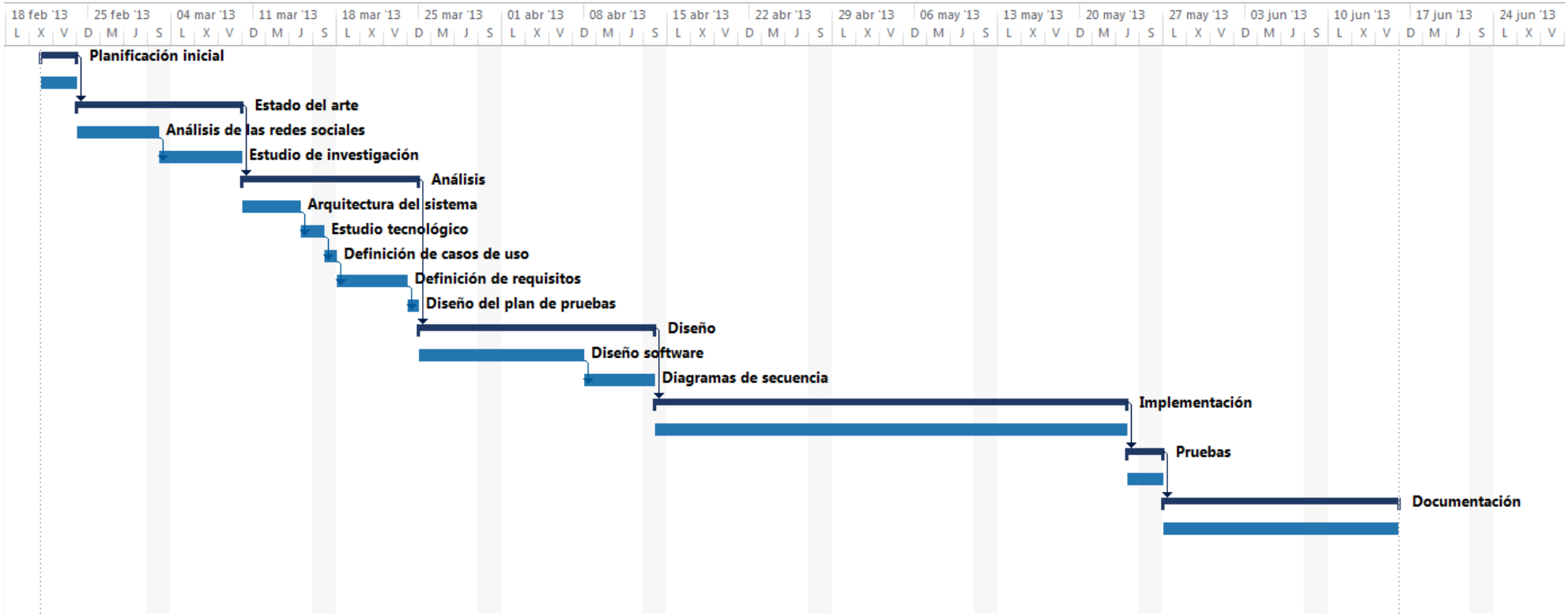

Figura 34. Diagrama de Gantt de la planificación inicial

1.2 Planificación real/final del trabajo de fin de grado

En esta sección se muestra el seguimiento que se ha realizado durante todo el trabajo de fin de grado, en el cual se encuentran los esfuerzos reales por cada una de las etapas del mismo. Después se realizará una comparación entre la planificación estimada y la real, así como una breve explicación sobre las diferencias encontradas.

La Tabla 10 muestra en detalle el desarrollo real del trabajo de fin de grado.

Desarrollo real			
Trabajo de fin de grado	**193 días**	**jue 21/02/2013**	**dom 01/09/2013**
Planificación inicial	**3 días**	**jue 21/02/2013**	**sáb 23/02/2013**
Estado del arte	**21 días**	**dom 24/02/2013**	**sáb 16/03/2013**
Análisis de las redes sociales	12 días	dom 24/02/2013	jue 07/03/2013
Estudio de investigación	9 días	vie 08/03/2013	sáb 16/03/2013
Análisis	**31 días**	**dom 17/03/2013**	**mar 16/04/2013**
Arquitectura del sistema	14 días	dom 17/03/2013	sáb 30/03/2013
Estudio tecnológico	7 días	dom 31/03/2013	sáb 06/04/2013
Definición de casos de uso	1 días	dom 07/04/2013	dom 07/04/2013
Definición de requisitos	7 días	lun 08/04/2013	dom 14/04/2013
Diseño del plan de pruebas	2 días	lun 15/04/2013	mar 16/04/2013
Diseño	**37 días**	**mié 17/04/2013**	**jue 23/05/2013**
Diseño software	25 días	mié 17/04/2013	sáb 11/05/2013
Diagramas de secuencia	12 días	dom 12/05/2013	jue 23/05/2013
Implementación	**63 días**	**vie 24/05/2013**	**jue 25/07/2013**
Pruebas	**7 días**	**vie 26/07/2013**	**jue 01/08/2013**
Documentación	**31 días**	**vie 02/08/2013**	**dom 01/09/2013**

Tabla 10. Desarrollo real del proyecto detallado

La Figura 35 muestra el diagrama de Gantt para el desarrollo real del trabajo de fin de grado.

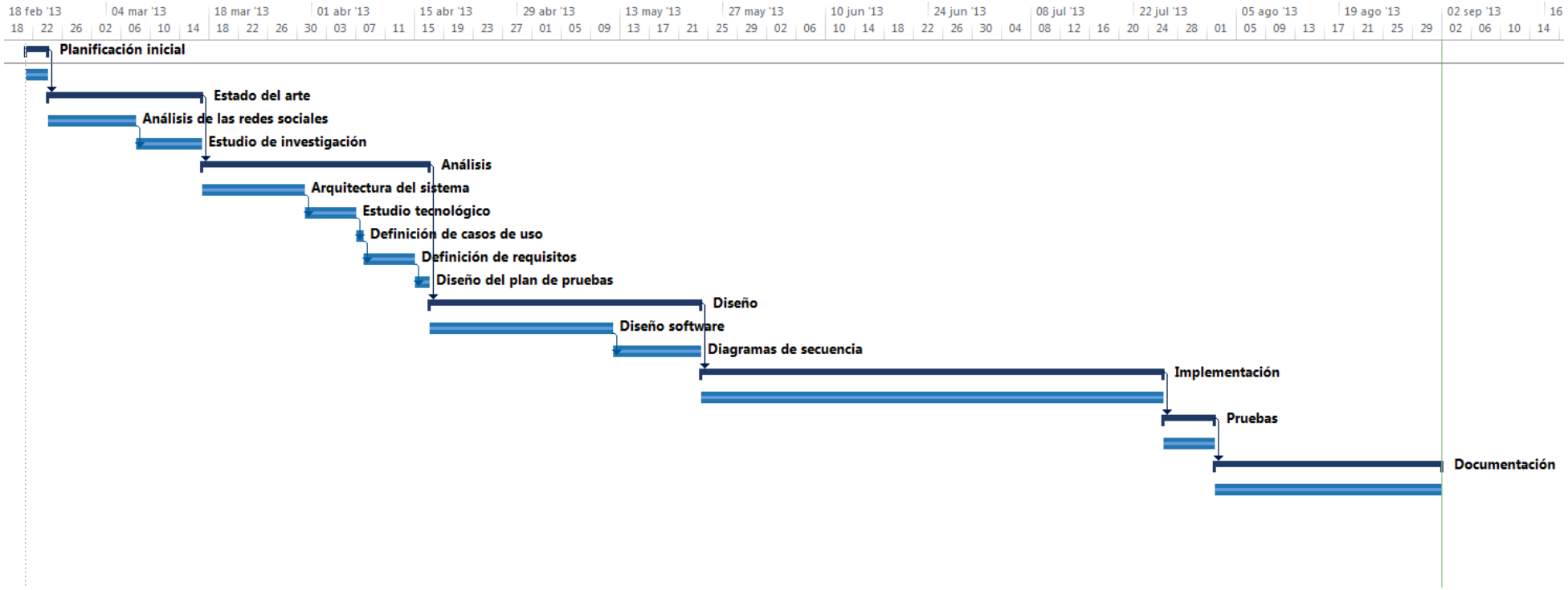

Figura 35. Diagrama de Gantt del desarrollo real

La Tabla 11 muestra un análisis numérico de la variación entre el tiempo planificado y el tiempo real transcurrido en el desarrollo del trabajo de fin de grado.

Análisis de desviaciones				
Etapa	**Planificado**	**Real**	**Diferencia**	**Desviación**
Trabajo de fin de grado	**115 días**	**193 días**	**78 días**	**40,4%**
Planificación inicial	**3 días**	**3 días**	**0 días**	**0,0%**
Estado del arte	**14 días**	**21 días**	**7 días**	**33,3%**
Análisis de las redes sociales	7 días	12 días	5 días	41,7%
Estudio de investigación	7 días	9 días	2 días	22,2%
Análisis	**15 días**	**31 días**	**16 días**	**51,6%**
Arquitectura del sistema	5 días	14 días	9 días	64,3%
Estudio tecnológico	2 días	7 días	5 días	71,4%
Definición de casos de uso	1 día	1 día	0 días	0,0%
Definición de requisitos	6 días	7 días	1 día	14,3%
Diseño del plan de pruebas	1 días	2 días	1 días	50,0%
Diseño	**20 días**	**37 días**	**17 días**	**45,9%**
Diseño software	14 días	25 días	11 días	44,0%
Diagramas de secuencia	6 días	12 días	6 días	50,0%
Implementación	**40 días**	**63 días**	**23 días**	**36,5%**
Pruebas	**3 días**	**7 días**	**4 días**	**57,1%**
Documentación	**20 días**	**31 días**	**11 días**	**35,5%**

Tabla 11. Análisis de desviaciones

Tal y como se puede apreciar, se realizó una estimación a la baja, ya que se ha completado el proyecto 78 días más tarde de lo previsto, lo que supone un 40% más de tiempo invertido de lo que se estimó. Esta importante diferencia es debida a las complicaciones surgidas, ya que se requirió un gran esfuerzo para definir correctamente el sistema y para solventar los problemas técnicos de implementación. Esto hizo que fuera necesario aplazar la fecha de entrega del trabajo de fin de grado, ya que la previsión era la de entregarlo en el llamamiento del mes de julio.

2. Medios técnicos empleados

En esta sección se listan las herramientas utilizadas para la elaboración del presente trabajo de fin de grado junto con una breve descripción de las mismas. Esta información se encuentra en la Tabla 12.

Herramientas utilizadas	
Herramienta	**Descripción**
Apple OSX 10.6 [35]	Sistema operativo utilizado sobre el que se han realizado las tareas de implementación y pruebas del trabajo de fin de grado.
Eclipse IDE for Java EE Developers [36]	Entorno de desarrollo web basada en Java utilizado para implementar el sistema.
Google Chrome [37]	Navegador web utilizado durante todo el proyecto para la búsqueda de información, realización de las pruebas en las redes sociales y realización de las pruebas del sistema.
Microsoft Office 2010 [38]	Suite de ofimática utilizada para la elaboración de la documentación del trabajo de fin de grado.
Microsoft Project 2013 [39]	Herramienta de gestión de proyectos utilizada para realizar la planificación inicial y un seguimiento del trabajo de fin de grado.
Microsoft Windows 7 Home Premium [40]	Sistema operativo utilizado sobre el que se han realizado las tareas de análisis, diseño y documentación del trabajo de fin de grado.
MySQL Workbench 6.0 [41]	Herramienta de gestión de bases de datos utilizada para acceder gráficamente a la base de datos del sistema.
TextWrangler [42]	Editor de texto simple utilizado para la creación de scripts de la base de datos.
Visual Paradigm for UML 10.2 [43]	Herramienta de modelado utilizada para crear todos los diagramas técnicos del trabajo de fin de grado.

Tabla 12. Herramientas utilizadas

La Tabla 13 muestra los medios físicos utilizados para el desarrollo del trabajo de fin de grado.

Medios físicos utilizados	
Equipo	**Descripción**
Sobremesa: Packard Bell iXtreme M5740	Ordenador de sobremesa sobre el que se han realizado las tareas de análisis, diseño y documentación del trabajo de fin de grado.
Portátil: Apple Macbook Pro 13-inch 2010	Ordenador portátil sobre el que se han realizado las tareas de implementación y pruebas del trabajo de fin de grado.
Impresora: HP Photosmart 5520	Impresora utilizada para la impresión de diversos documentos relacionados con el trabajo de fin de grado.
Teléfono: Samsung Galaxy Nexus 16GB	Teléfono móvil utilizado como medio de comunicación, agenda y lector de correos.

Tabla 13. Medios físicos utilizados

3. Análisis económico del trabajo de fin de grado

En esta sección se realiza un análisis del esfuerzo económico que ha supuesto el trabajo de fin de grado. En él se incluyen la metodología de estimación de costes usada, el presupuesto inicial y el coste real del trabajo.

Se ha utilizado para esta sección la plantilla proporcionada por la Universidad Carlos III de Madrid [44].

3.1 Metodología de estimación de costes

La estimación de costes ha tenido en cuenta costes directos y costes indirectos.

Los costes directos son aquellos que están relacionados directamente con el desarrollo del trabajo de fin de grado, como los equipos, las herramientas software, la mano de obra, los materiales consumibles, las dietas y los gastos de desplazamiento. Los gastos de equipos y herramientas software se han calculado en base al precio de venta al público, los gastos de mano de obra considerando que el trabajador pertenece a una empresa, es decir, que no es autónomo, y los gastos de desplazamiento en función de los kilómetros recorridos.

Los costes indirectos representan los costes que no tienen una relación directa con el trabajo de fin de grado pero que se deben incurrir, como los gastos de teléfono y la conexión a internet. En base a la plantilla proporcionada, los costes indirectos se calcularán como un 20% de los costes directos.

3.2 Presupuesto inicial

En esta sección se detalla el presupuesto inicial previsto para la realización del trabajo de fin de grado. El 21% de IVA no ha sido considerado para las estimaciones de costes, sino que se ha añadido al final

3.2.1 Gastos de equipos

Los equipos utilizados durante el trabajo de fin de grado fueron dos ordenadores, una impresora y un teléfono móvil. Se considera un período de deprecación para los ordenadores y la impresora es el utilizado en la Administración General, 36 meses, mientras que el del teléfono es el tiempo transcurrido entre el lanzamiento de modelos más novedosos. La Tabla 14 muestra el desglose de los gastos en equipos.

Gastos de equipos				
Equipo	**Coste (sin IVA)**	**Dedicación**	**Período de deprecación**	**Coste imputable**
Sobremesa: Packard Bell iXtreme M5740	661,16 €	3,87 meses	36 meses	71,07 €
Portátil: Apple Macbook Pro 13-inch 2010	1.206,61 €	3,87 meses	36 meses	129,71 €
Impresora: HP Photosmart 5520	78,51 €	3,87 meses	36 meses	8,43 €
Teléfono: Samsung Galaxy Nexus 16GB	495,87 €	3,87 meses	24 meses	79,96 €
			Coste total imputable	**287,17 €**

Tabla 14. Gastos de equipos

3.2.2 Gastos de software

La Tabla 12 mostraba la lista de software utilizado para el desarrollo del trabajo de fin de grado en la sección 2 de este anexo. En la Tabla 15 se pueden apreciar los costes asociados a cada uno de ellos. Únicamente se muestran las herramientas que no son software libre y por tanto suponen un coste.

Gastos de software				
Herramienta	**Coste (sin IVA)**	**Dedicación**	**Período de deprecación**	**Coste imputable**
Apple OSX 10.6	30,00 €	3,87 meses	36 meses	3,22 €
Microsoft Office 2010	98,34 €	3,87 meses	36 meses	10,57 €
Microsoft Project 2013	635,53 €	3,87 meses	36 meses	68,32 €
Microsoft Windows 7 Home Premium	107,43 €	3,87 meses	36 meses	11,55 €
Visual Paradigm for UML 10.2	438,44 €	3,87 meses	36 meses	47,13 €
			Coste total imputable	**140,79 €**

Tabla 15. Gastos de software

3.2.3 Gastos de personal

La Tabla 16 muestra los gastos de personal previstos a incurrir en el desarrollo del trabajo de fin de grado. La dedicación está calculada en base a una jornada de 3 horas diarias durante 115 días. El coste hombre mes está tomado de la plantilla proporcionada por la Universidad Carlos III de Madrid, añadiéndosele un 28,3% de importe que irá destinado a la Seguridad Social.

Gastos de personal					
Recurso	**Dedicación**	**Coste hombre/mes**	**Coste bruto**	**Seguridad Social**	**Coste total**
Ingeniero	2,628 hombre/mes	2.694,39 €	7.082,40 €	2.004,39 €	9.086,79 €
				Coste total imputable	**9.086,79 €**

Tabla 16. Gastos de personal

3.2.4 Gastos de consumibles

Se han considerado también los gastos de materiales consumibles. A continuación, la Tabla 17 detalla estos gastos. Se han considerado como materiales consumibles los cartuchos de impresora y los materiales de oficina, como folios, carpetas, bolígrafos y grapadoras entre otros.

Gastos de consumibles			
Material	**Coste unitario (Sin IVA)**	**Cantidad**	**Coste total**
Cartuchos de impresora	29,75 €	1	29,75 €
Material de oficina	20,66 €	1	20,66 €
		Coste total imputable	**50,41 €**

Tabla 17. Gastos de consumibles

3.2.5 Gastos de viajes y dietas

Los gastos por desplazamiento y las dietas están considerados también en el presupuesto, ya que se han realizado viajes para reuniones con el cliente, que en este caso particular se considera como tal a la tutora del presente trabajo de fin de grado. Este gasto se ha calculado en base al coste del transporte público utilizado, el cual supone 2€ de ida y otros 2€ de vuelta. Las dietas se contabilizan por cada día que se ha mantenido una reunión, y se calcula como 6€ por día. La Tabla 18 muestra en detalle los gastos de viajes y dietas.

Gastos de consumibles			
Concepto	**Coste unitario (Sin IVA)**	**Cantidad**	**Coste total**
Autobús a Leganés	3,31 €	8	26,45 €
Dietas	4,96 €	8	39,67 €
		Coste total imputable	**66,12 €**

Tabla 18. Gastos de viajes y dietas

3.2.6 Costes directos

Esta sección presenta un resumen de todos los costes imputables a cada uno de los gastos considerados anteriormente. La Tabla 19 muestra el resultado de los costes directos.

Costes directos	
Concepto	**Coste**
Gastos de equipos	287,17 €
Gastos de software	140,79 €
Gastos de personal	9.086,79 €
Gastos de consumibles	50,41 €
Gastos de viajes y dietas	66,12 €
Coste total	**9.631,28 €**

Tabla 19. Costes directos

3.2.7 Costes indirectos

En esta sección se calculan los costes indirectos. Éstos son calculados en base a los costes directos como un 20% de los mismos. Así pues, los costes indirectos estimados son 1.926,26 €.

3.2.8 Estimación de costes

En esta sección se presenta la estimación de costes, obtenida de sumar los costes directos más los indirectos y aplicarles el 21% de IVA. La Tabla 20 muestra la estimación de costes calculada.

Estimación de costes	
Concepto	**Coste**
Gastos de equipos	287,17 €
Gastos de software	140,79 €
Gastos de personal	9.086,79 €
Gastos de consumibles	50,41 €
Gastos de viajes y dietas	66,12 €
Gastos directos	9.631,28 €
Gastos indirectos	1.926,26 €
Total (Sin IVA)	**11.557,54 €**
IVA (21%)	2.427,08 €
Total	**13.984,62 €**

Tabla 20. Costes directos

3.3 Presupuesto para el cliente

En esta sección se detalla el presupuesto presentado al cliente, donde se incluye la estimación de costes calculada en la sección anterior. A esta estimación de costes se le añaden un porcentaje de riesgos más otro porcentaje de beneficios a obtener.

El porcentaje de riesgos será de un 15%, de acuerdo con la experiencia tras anteriores estimaciones de costes realizadas fuera del ámbito del trabajo de fin de grado.

El porcentaje de beneficios se establecerá en un 15%, puesto que será el único beneficio que se obtendrá con la realización de este trabajo de fin de grado. La herramienta se pondrá a disposición de todos los usuarios de forma gratuita en el mercado de aplicaciones integrado en Facebook.

La aplicación tiene un gran interés público, ya que actualmente la privacidad en las redes sociales es crítica. Tal y como se ha explicado y demostrado en los Capítulos 1 y 2 del presente documento, las herramientas existentes son insuficientes para proporcionar anonimato en las redes sociales, además de gestionar la co-propiedad de los álbumes. Gracias a este sistema se ha conseguido mejorar considerablemente los actuales proporcionando anonimato tanto en el proceso de votación como en el acceso a los álbumes, a la vez que un sistema de gestión de la co-propiedad.

La Tabla 21 detalla el presupuesto que será entregado al cliente. *Nota: En ella, se muestran también el margen de riesgo y los beneficios. Se han incluido únicamente por interés analítico. El presupuesto que se presentaría a un cliente real no incluiría estos datos, se añadirían sobre el total de los costes*.

Presupuesto	
Concepto	**Coste**
Gastos de equipos	287,17 €
Gastos de software	140,79 €
Gastos de personal	9.086,79 €
Gastos de consumibles	50,41 €
Gastos de viajes y dietas	66,12 €
Gastos directos	9.631,28 €
Gastos indirectos	1.926,26 €
Total costes (Sin IVA)	**11.557,54 €**
Riesgo (15%)	1.733,63 €
Total con riesgo (Sin IVA)	**13.291,17 €**
Beneficios (15%)	1.993,68 €
Total con beneficios (Sin IVA)	**15.284,85 €**
IVA (21%)	3.209,82€
Total	**18.494,66 €**

Tabla 21. Presupuesto

3.4 Coste final y análisis de la desviación

En esta sección se presentan los costes reales incurridos en el trabajo de fin de grado junto con un análisis de la desviación producida entre los costes estimados y los costes finales.

La Tabla 22 muestra el análisis detallado de éstos junto con la desviación. El coste real es calculado en base a las mismas consideraciones que el estimado, variando los valores imputados a cada concepto en función a la diferencia de días, viajes, cantidades, etc.

Costes finales				
Concepto	**Coste estimado**	**Coste real**	**Variación**	**Desviación**
Gastos de equipos	287,17 €	436,19 €	149,02 €	51,89 %
Gastos de software	140,79 €	233,93 €	93,14 €	66,15 %
Gastos de personal	9.086,79 €	15.170,86 €	6.084,07 €	66,95 %
Gastos de consumibles	50,41 €	46,28 €	-4,13 €	-8,19 %
Gastos de viajes y dietas	66,12 €	49,62 €	-16,50 €	-24,95 %
Gastos directos	9.631,28 €	15.936,88 €	6.305,60 €	65,47 %
Gastos indirectos	1.926,26 €	3.187,38 €	1.261,12 €	65,47 %
Total (Sin IVA)	**11.557,54 €**	**19.124,26 €**	**7.566,72 €**	**65,47 %**
Riesgo (15%)	1.733,63 €	1.733,63 €	0 €	0 %
Total con riesgo (sin IVA)	**13.291,17 €**	**20.857,89 €**	**7.566,72 €**	**56,93 %**
Beneficios (15%)	1.993,68 €	1.993,68 €	0 €	0 %
Total con beneficios (sin IVA)	**15.284,85 €**	**22.851,57 €**	**7.566,72 €**	**49,50 %**
IVA (21%)	3.209,82€	4.798,83 €	1.589,01 €	49,50 %
Total	**18.494,66 €**	**27.650,39 €**	**9.155,73 €**	**49,50 %**

Tabla 22. Costes finales

Tal y como se aprecia en la Tabla 22, existe una gran desviación del 49,50% sobre el presupuesto estimado, lo que suponen 9.155,73 € de variación sobre el total. La causa de esta importante diferencia son los retrasos sufridos a lo largo de todas las fases del proyecto. Al aumentarse el tiempo del proyecto casi al doble de lo estipulado, de 115 días a 193 días, se ha producido un importante aumento que ha sido más acusado en los gastos de personal, que además supone un gran aumento de costes de Seguridad Social. Todo ello en conjunto repercute en que cuando se aplica el IVA el valor sobre el que hay que aplicarlo es un 65,47% mayor que lo presupuestado, lo que hace que aumente aún más la cifra.

Tal y como continúa mostrando la tabla, el capital de riesgo aportado por el cliente y los beneficios obtenidos se mantienen constantes, ya que estas cifras no pueden variar respecto a las presupuestadas. Realizando operaciones sobre el total sin IVA, se puede observar el balance general económico. El gasto total a afrontar es de 19.124,26€, habiendo aportado el cliente 11.554,54€. La diferencia entre ambos es de 7.566,72€. Como la cantidad aportada no es suficiente, se ha hecho necesario utilizar el fondo de riesgo (1.733,63€) para afrontar el gasto. El balance en este punto es de una pérdida de 5833,09€, haciéndose necesario utilizar el margen de beneficios (1.993,68€) como medio para asumir esta cantidad. Tras aportar este capital, la cifra desciende hasta los 3839,41€, haciéndose necesario aportar esta cantidad de los fondos propios.

La envergadura del trabajo de fin de grado ha hecho que las estimaciones hayan sido erróneas, ya que no se ha realizado un proyecto de similares dimensiones anteriormente y se ha tendido a subestimar en tiempo. El porcentaje de riesgo ha sido completamente erróneo ya que se han producido muchas más dificultades que podrían surgir según lo calculado.

Anexo 2

Manual de usuario

1. Introducción

CANONYM (*Co-ownership & Anonymity*) es una aplicación de Facebook gratuita y que permite a los usuarios gestionar la co-propiedad de sus álbumes de fotos mediante un proceso de votación de la misma totalmente anónimo. Tras la realización de este proceso, el sistema autoriza, o no autoriza, a visualizar un álbum a los usuarios que posean una credencial anónima mediante un proceso de comprobación de credenciales que mantiene el anonimato del usuario.

Este manual debe ser una referencia para los usuarios de la aplicación para su correcto uso.

2. Requisitos previos e instalación

La parte de la votación de la política de CANONYM es una aplicación web, y por lo tanto no se requiere ningún requisito para su instalación, basta con acceder a ella desde el centro de aplicaciones de Facebook.

Sin embargo, la parte del acceso anónimo a los álbumes utiliza un programa Java en la máquina del usuario, por lo que se requerirá que el usuario tenga instalado Java en su versión 1.6 para poder utilizar esta parte. Seguidamente el usuario deberá descargar el programa cliente de las credenciales anónimas y utilizarlo cuando la aplicación web se lo indique.

En general, no existen limitaciones técnicas específicas para la utilización del sistema ya que no se requiere más que un ordenador, sin importar el sistema operativo, con acceso a Internet. Como datos de referencia se darán a continuación las características recomendables:

- Memoria RAM: 1 GB.
- Memoria de vídeo: 16 MB.
- Espacio en disco: 10 MB.

3. Ejecución y funcionamiento

Su ejecución se inicia al seleccionar la aplicación en Facebook, haciendo click en CANONYM, encontrado en la lista de aplicaciones.

Al iniciarse se muestra la pantalla principal que se puede apreciar en la Figura donde se le indica al usuario que debe estar autenticado en Facebook y se le muestra un botón de autenticación por si no lo está. Haciendo click en "Enter" se accederá al menú principal de la aplicación.

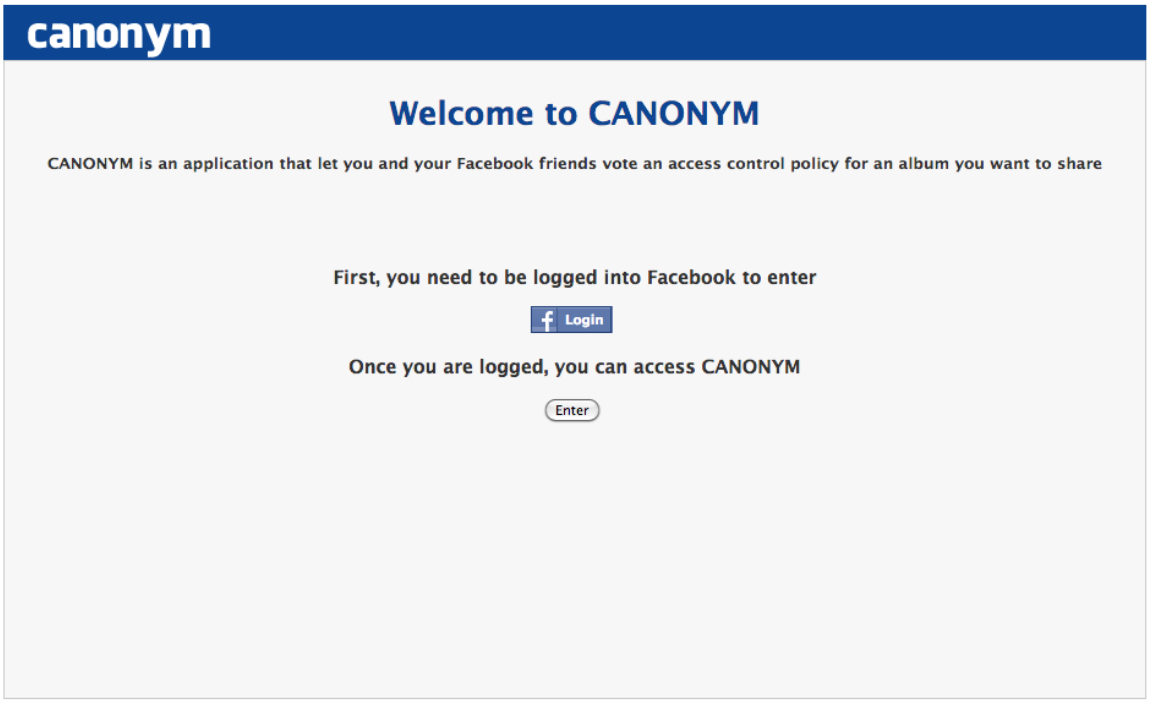

Figura 36. Pantalla principal de CANONYM

La Figura 37 muestra el menú principal de la aplicación, donde se encuentran tres secciones. "Share new album" se utiliza para que un propietario cree un nuevo proceso de votación de la política de control de acceso para un álbum que seleccione. "Manage your shared albums" se utiliza para que los co-propietarios voten la política de control de acceso para un álbum que un propietario ha elegido. Finalmente, "Last step" es el último paso que todos ellos deben dar para que la política pueda ser computada y asignada al álbum compartido.

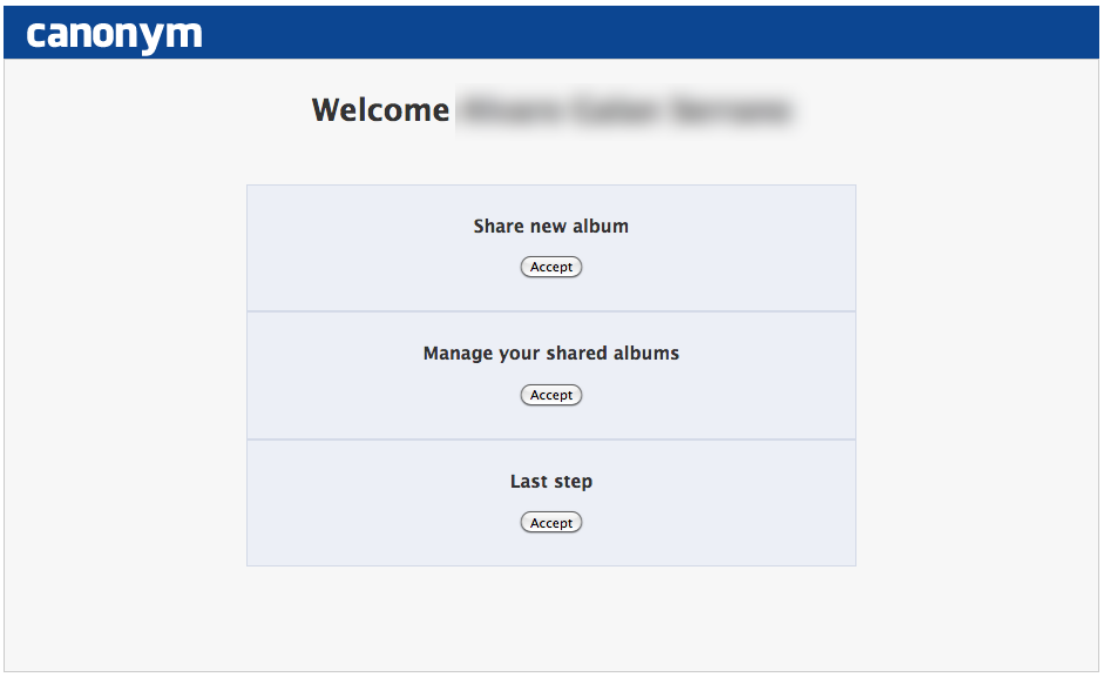

Figura 37. Menú principal en CANONYM

3.1 Compartir nuevo álbum

Si se selecciona la primera opción de la Figura 37 comenzará el proceso de creación de un nuevo álbum sobre el que votar la política. Este paso lo debe escoger el propietario de un álbum que desee gestionar su co-propiedad. Tras seleccionar "Accept" aparecerá la ventana que se muestra en la Figura 38, donde el propietario debe seleccionar el álbum que desea compartir junto con una previsualización del mismo.

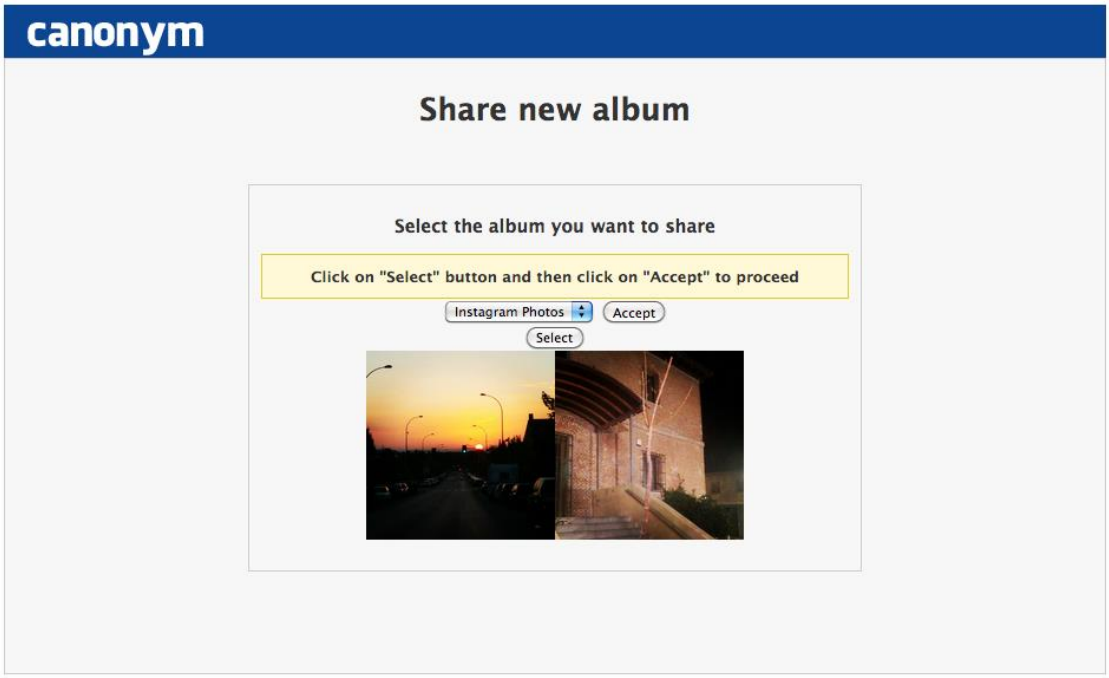

Figura 38. Seleccionar álbum en CANONYM

Tras hacer click en “Select” para fijar el álbum y en “Accept” para avanzar en el proceso, aparecerá la ventana representada en la Figura 39, donde se deben seleccionar los amigos con los que compartir el álbum. Tras pulsar “Accept” se pasará al paso siguiente.

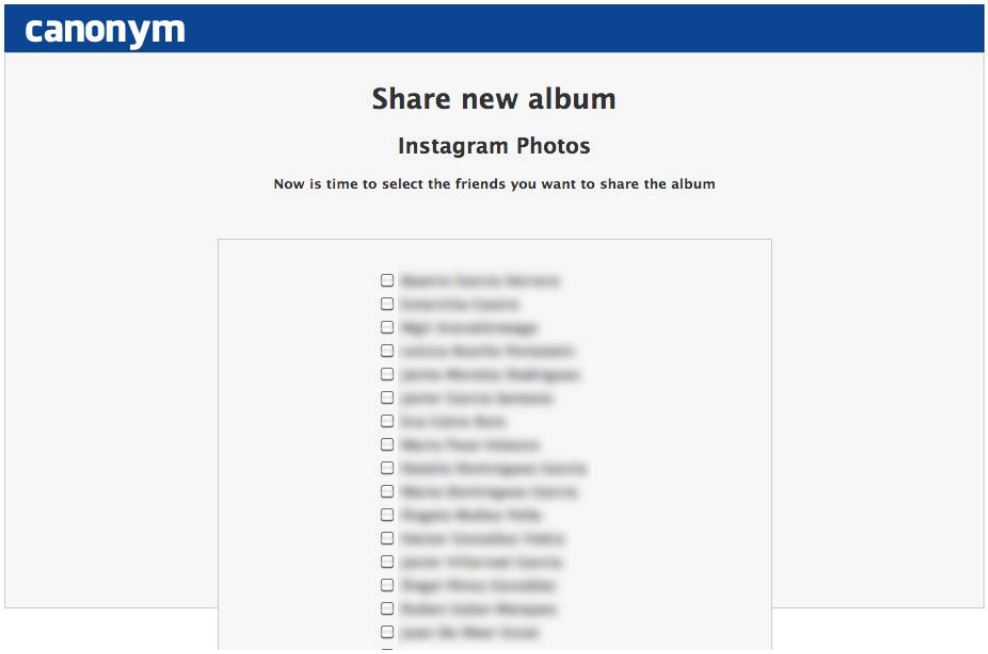

Figura 39. Seleccionar amigos en CANONYM

Una vez se ha llegado a este punto, es el momento en el que el propietario del álbum vote la política de control de acceso que desea para su álbum. La Figura 40 muestra la ventana de votación. Tras pulsar en “Compute” para generar los valores que el usuario deberá apuntar (recuadrados en amarillo) y pulsar en “Accept” se pasará a la última fase de esta parte del proceso.

En este momento es necesario notificar a los co-propietarios del álbum, enviándoles un mensaje de Facebook con un código de autenticación. Aparece la ventana de la Figura 41 donde se debe pulsar en “Send” para comenzar a enviar los mensajes. Se abrirán cuadros de diálogo de Facebook donde se muestra uno a uno el mensaje que va a ser enviado al co-propietario (Figura 42). Pulsando en “Enviar” uno tras otro se habrán enviado los mensajes necesarios. En este momento vuelve a aparecer la ventana de la Figura 41 donde, pulsando “Accept” habrá finalizado el proceso y se redirigirá al usuario al menú principal (Figura 37).

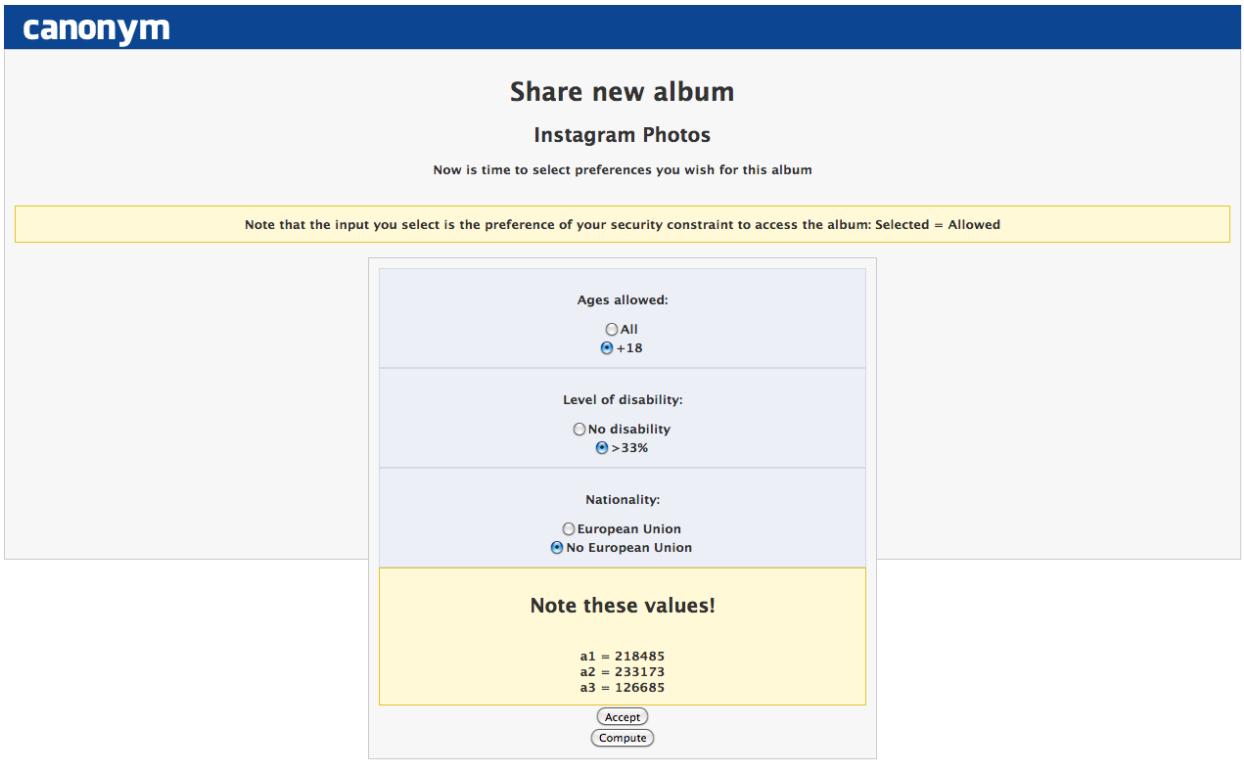

Figura 40. Seleccionar preferencias en CANONYM (1)

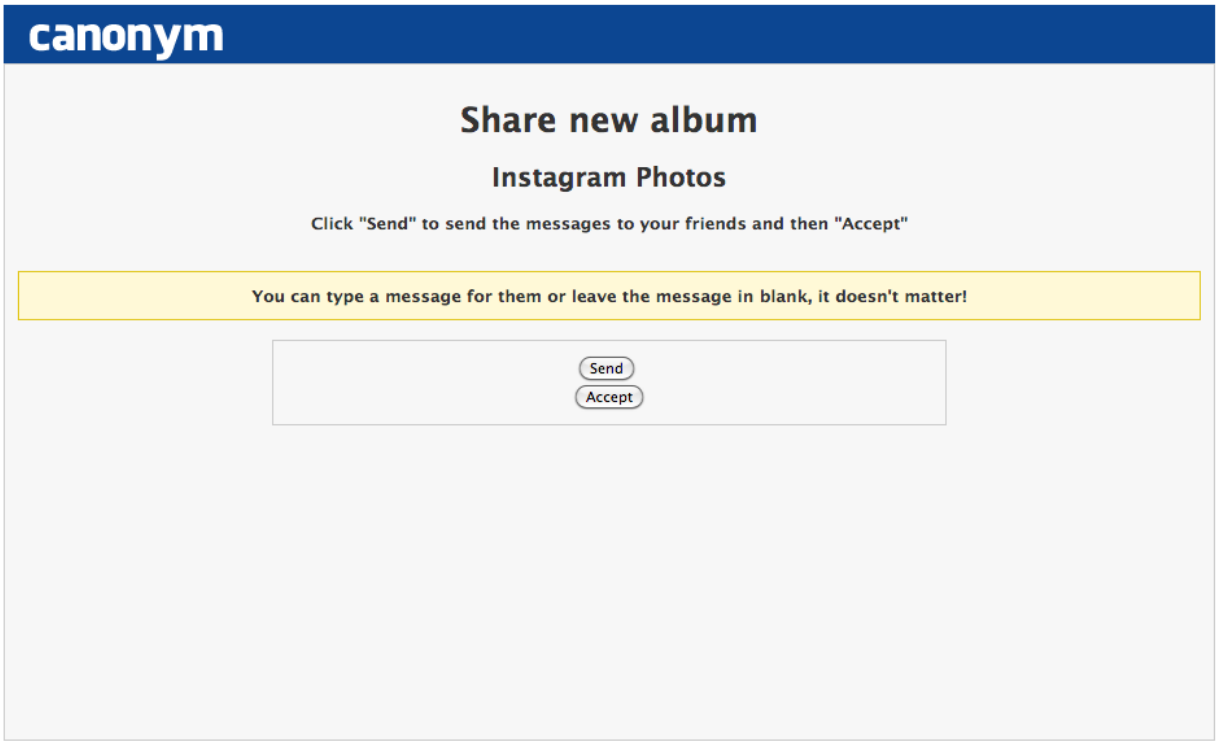

Figura 41. Enviar mensajes en CANONYM (1)

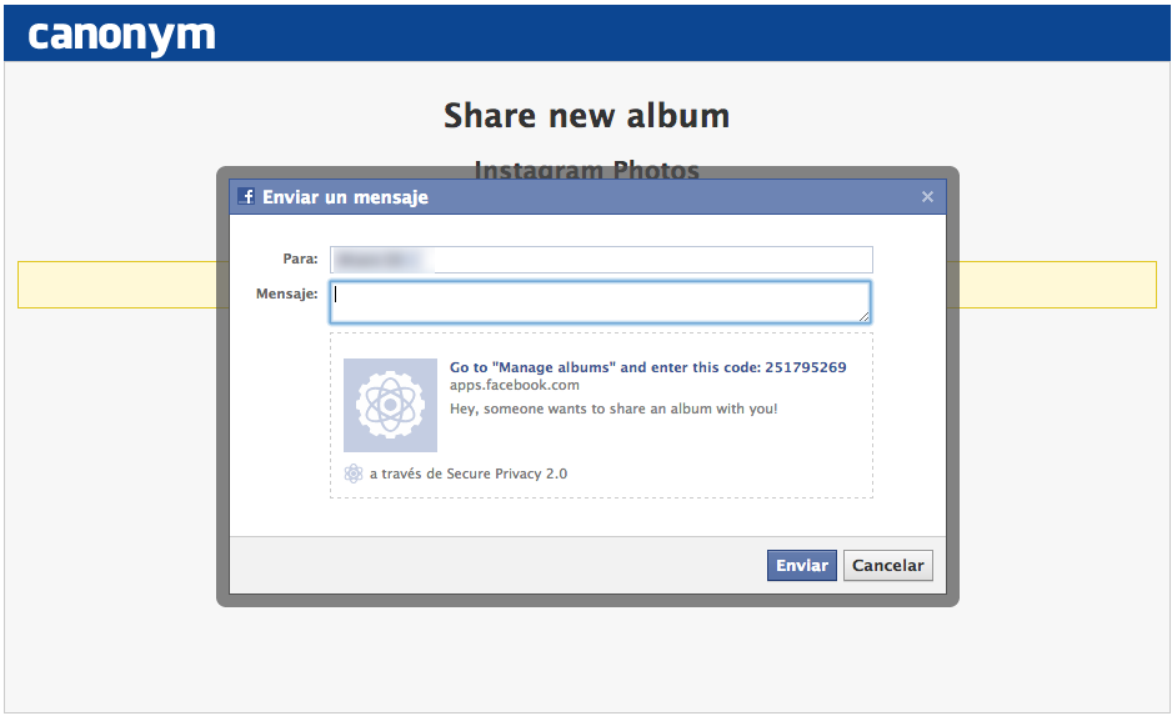

Figura 42. Enviar mensajes en CANONYM (2)

3.2 Votar un álbum como co-propietario

Para votar un álbum como co-propietario es necesario haber recibido un mensaje que indique la necesidad de su intervención en el proceso de votación.

En primer lugar, debe entrar a la aplicación (Figura 36) y seleccionar la segunda opción del menú principal (Figura 37). Una vez se encuentra en la ventana que aparece en la Figura 43, deberá introducir el código de autenticación recibido en el mensaje de Facebook que le envió el propietario del álbum y pulsar "Accept" para pasar al siguiente paso.

En este momento se mostrará una previsualización del álbum que se desea compartir, mostrado en la Figura 44. Si se pulsa "Accept" se dará paso a la ventana de votación de la política de control de acceso que desea el co-propietario. La Figura 45 contiene la página de votación. Tras hacer click en "Compute" se mostrarán los valores que el co-propietario debe apuntar. Haciendo click en "Accept" se pasará al siguiente paso.

Si aún quedan más co-propietarios por realizar la votación se volverá al menú principal de la Figura 37. En cambio, si el co-propietario que está realizando la votación es el último de todos, se mostrará una ventana para enviar mensajes a todos los participantes avisándoles de que han terminado de votar todos (Figura 46). Se mostrará la pantalla de la Figura 47. Al pulsar "Send" se abrirá el cuadro de diálogo de envío de mensajes de Facebook. Tras hacer click en "Enviar mensaje" para todos los participantes se cerrará el diálogo y se volverá a la pantalla de la Figura 46. En este mensaje se envía un código de autenticación y se les indica de que deben acceder a la última opción del menú principal para completar el proceso. Al finalizar se volverá al menú principal (Figura 37).

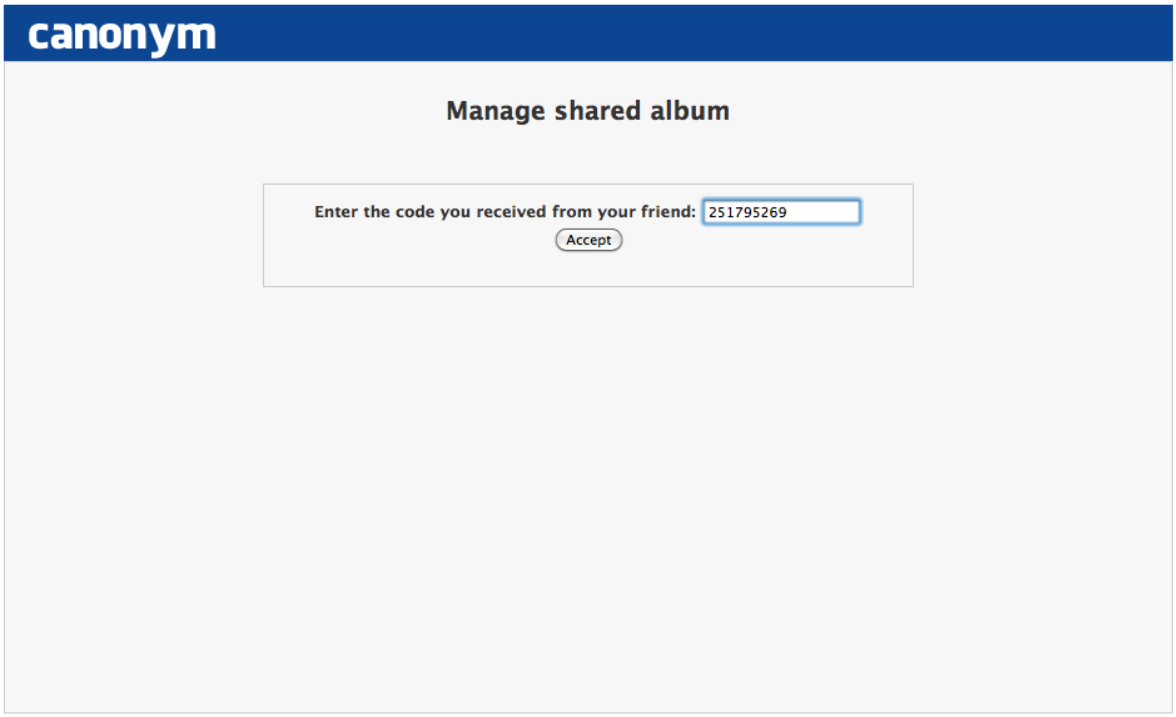

Figura 43. Código de autenticación en CANONYM

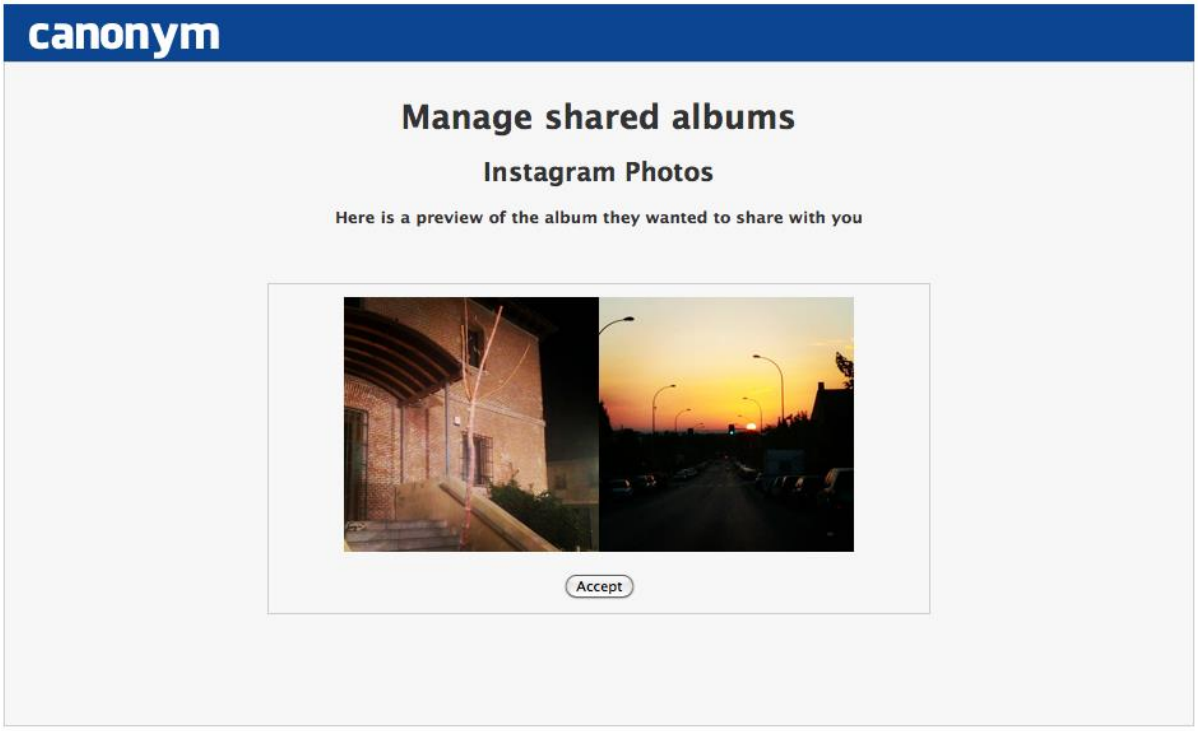

Figura 44. Previsualización en CANONYM

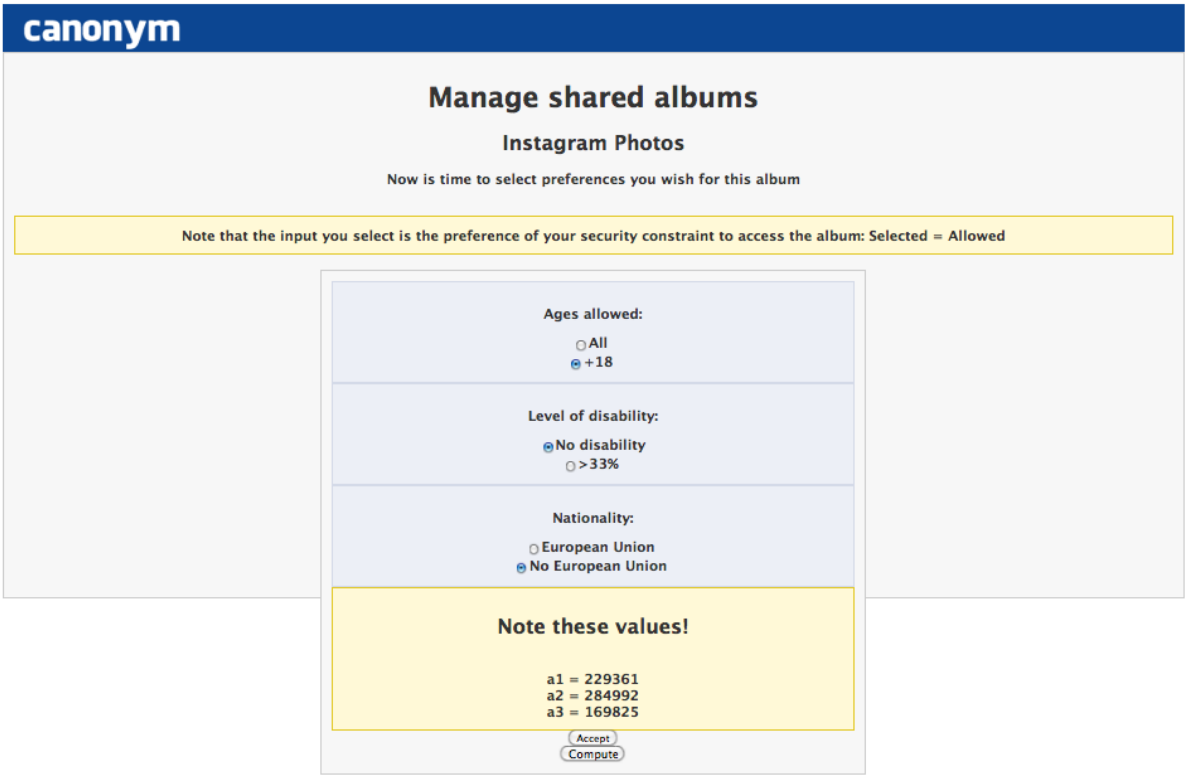

Figura 45. Seleccionar preferencias en CANONYM (2)

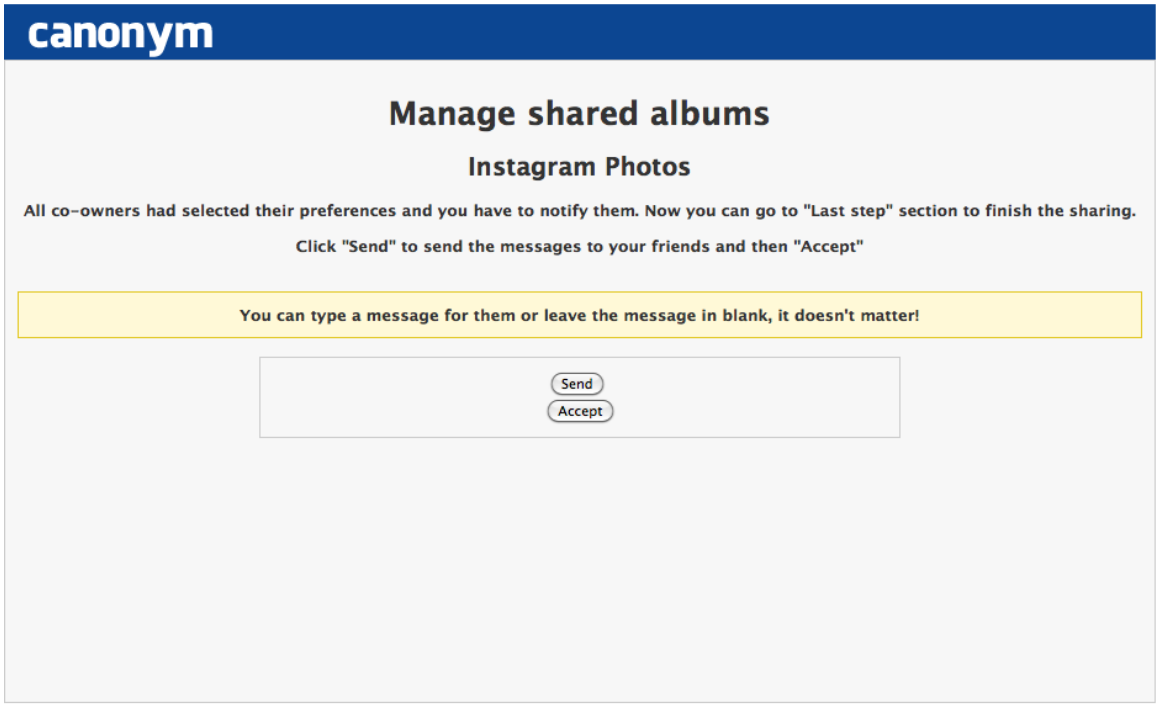

Figura 46. Enviar mensajes en CANONYM (3)

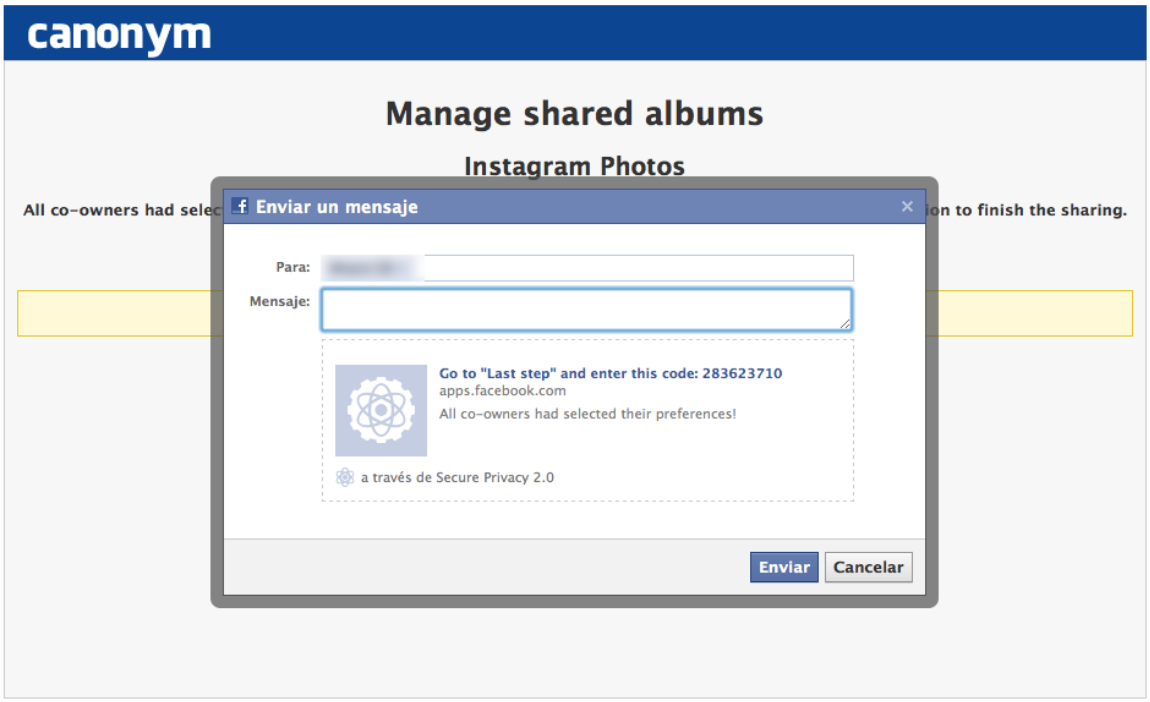

Figura 47. Enviar mensajes en CANONYM (4)

3.3 Último paso del proceso de votación

Una vez todos los participantes han escogido sus preferencias, es necesario que todos introduzcan los valores que han apuntado escogiendo la tercera opción del menú principal (Figura 37).

Tras hacer click en “Accept”, se abrirá una página para introducir el código de autenticación recibido por mensaje de Facebook, de igual forma que se observa en la Figura 43. Tras realizarse la autenticación al pulsar en “Accept”, se mostrará una ventana para introducir los valores que se apuntaron. La Figura 48 muestra esta ventana donde, una vez se introduzcan los datos, se pulsará en “Compute” y después en “Accept” para enviar los datos necesarios al servidor.

Si el usuario era el último de todos por enviar estos datos, el sistema le notificará que se ha computado correctamente la política de control de acceso, mostrando la ventana que aparece en la Figura 49.

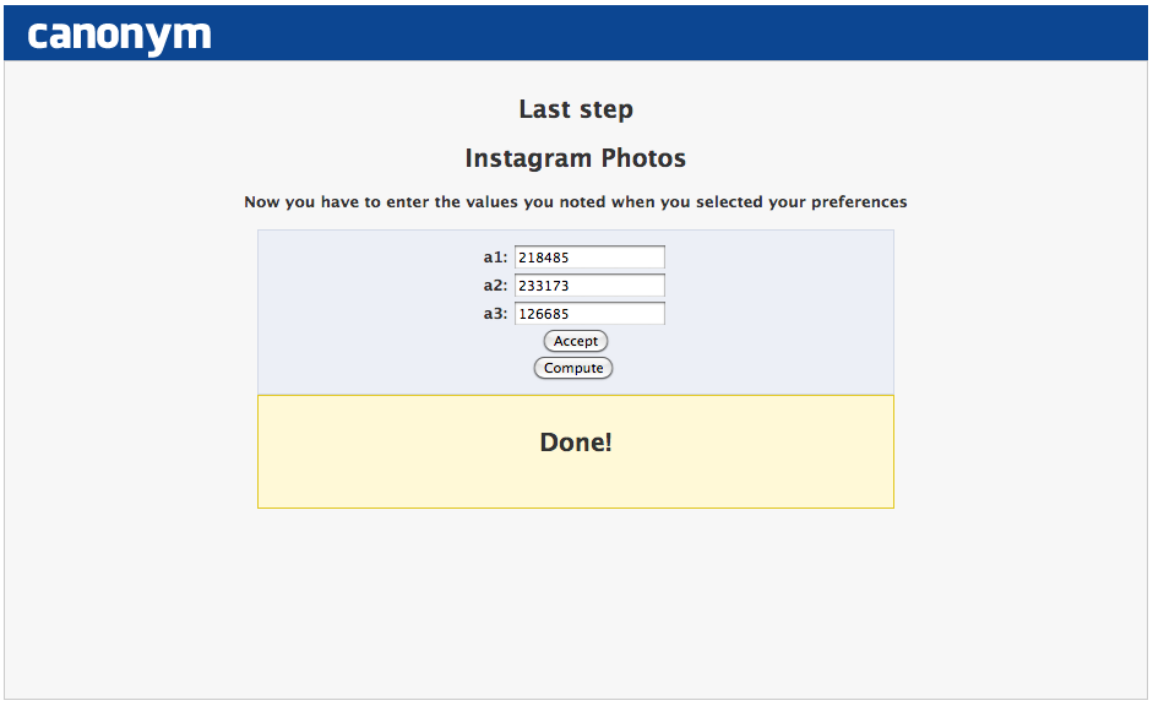

Figura 48. Introducir valores en CANONYM

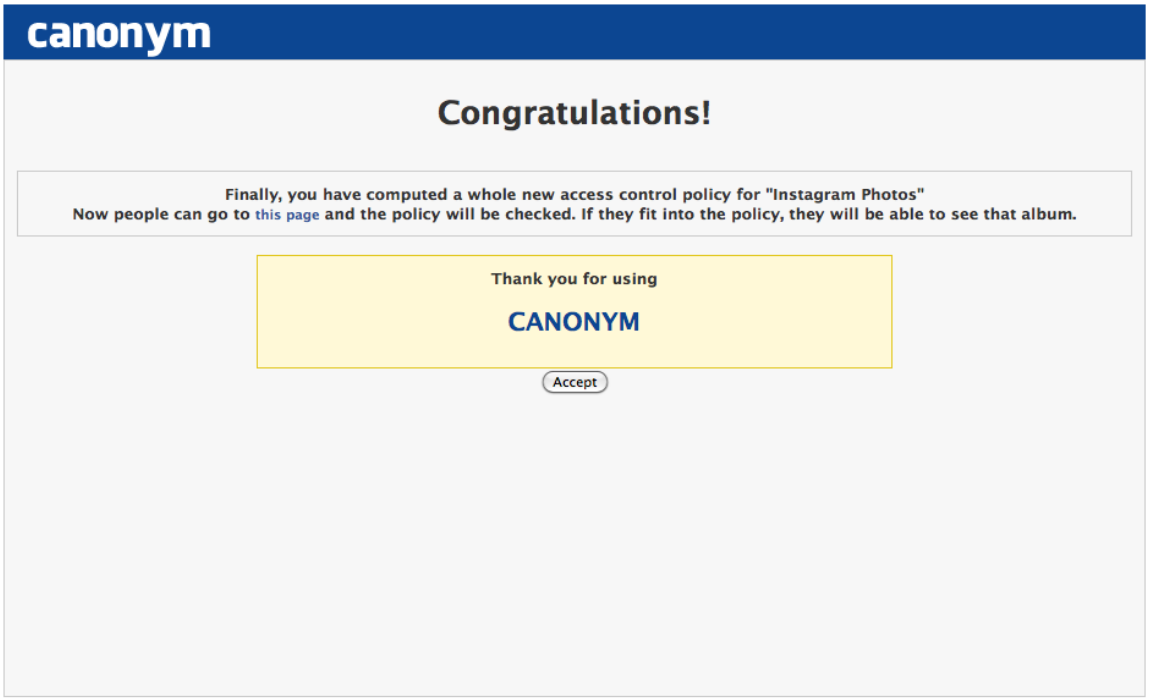

Figura 49. Fin del proceso en CANONYM

3.4 Acceso anónimo a los álbumes

En la Figura 49 se puede apreciar que existe un enlace sobre las letras “this page”, que redirecciona a la página de acceso a los álbumes, que se encuentra fuera de Facebook ya que no se requiere que el usuario posea una cuenta en esta red social. Esta ventana se muestra en la Figura 50 donde, tras pulsar en “Accept”, se pasará al siguiente paso del acceso anónimo.

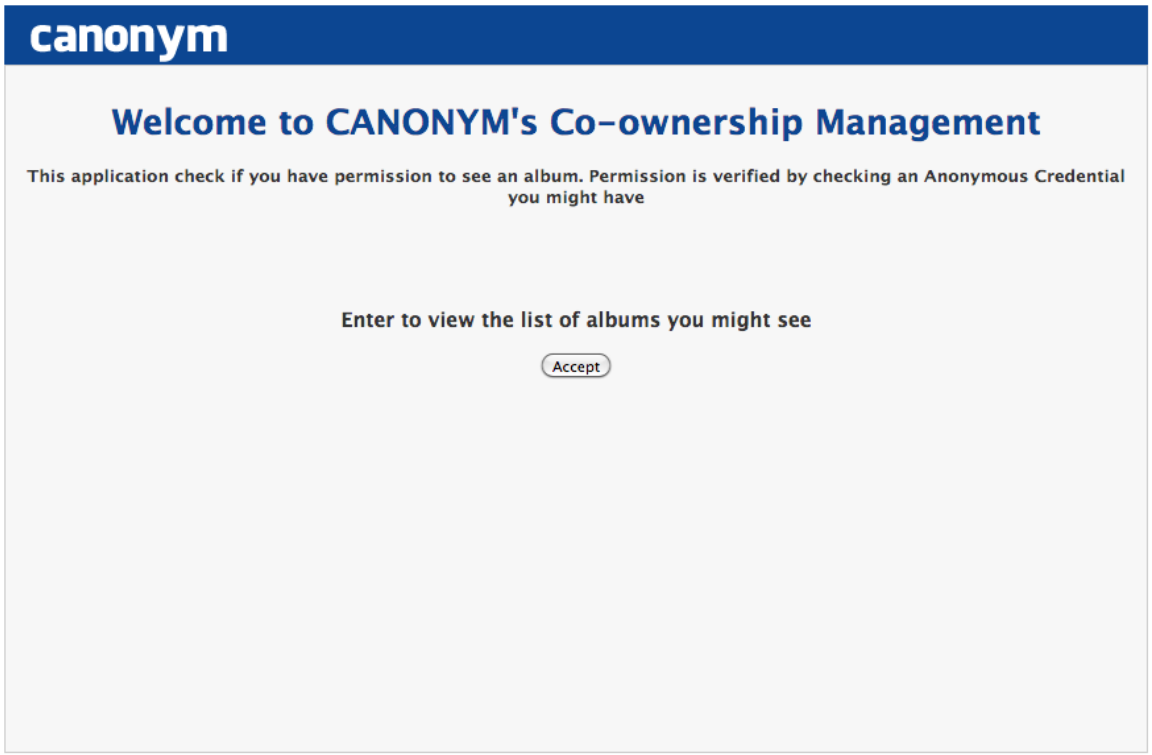

Figura 50. Bienvenida al acceso anónimo en CANONYM

A continuación se mostrará una pantalla donde se ofrece la lista de álbumes a los que se puede acceder a visualizar, que son los previamente compartidos en el sistema, junto con la política de control de acceso. En la Figura 51 se muestra esta ventana en la cual se debe seleccionar uno de ellos y pulsar en “Select” para pasar a verificar la credencial.

A continuación se muestra la ventana de chequeo de credenciales que aparece en la Figura 52. La aplicación indica que es necesario ejecutar el programa de chequeo local para introducir los ficheros que se indican. Si se ejecuta el programa “check.jar” que se provee al usuario y se introduce la credencial en la misma carpeta que él, el programa generará varios ficheros, que serán los que se deben introducir en la aplicación. Tras seleccionar los ficheros en la ventana de la Figura 52 y hacer click en “Upload”, comenzará un proceso de verificación de los ficheros totalmente transparente al usuario donde, si el resultado es positivo, aparecerá el álbum que se desea visualizar tal y como aparece en la Figura 53.

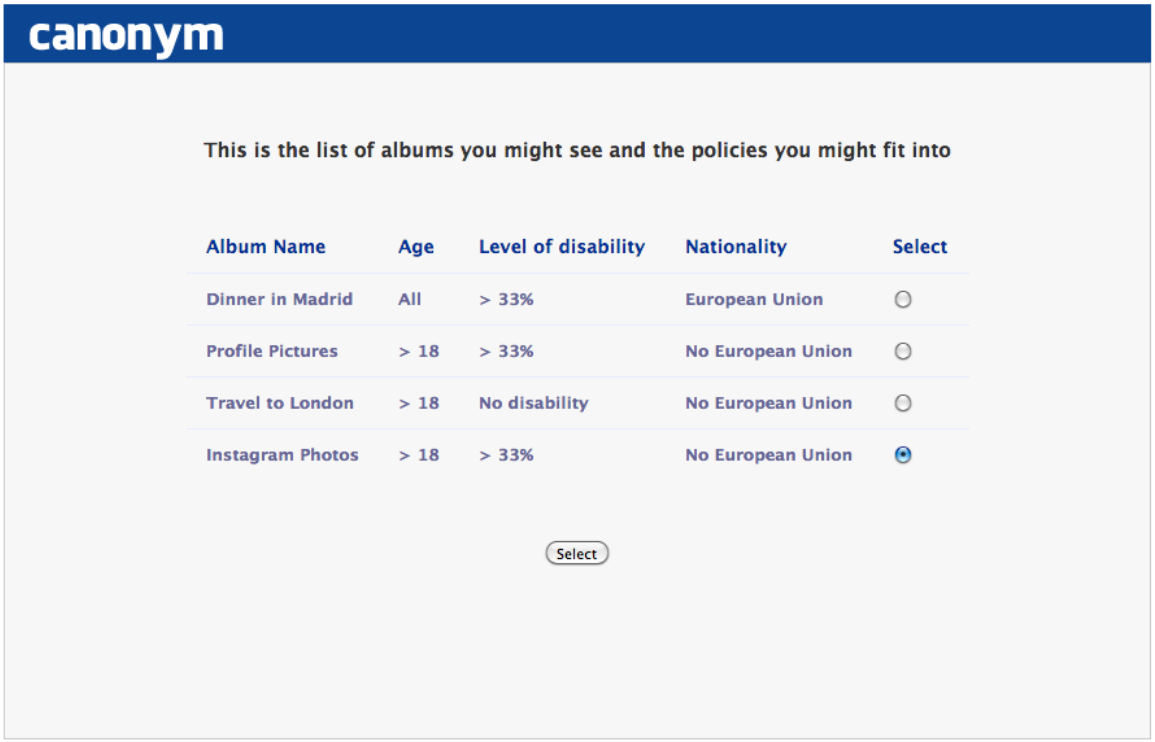

Figura 51. Lista de álbumes en CANONYM

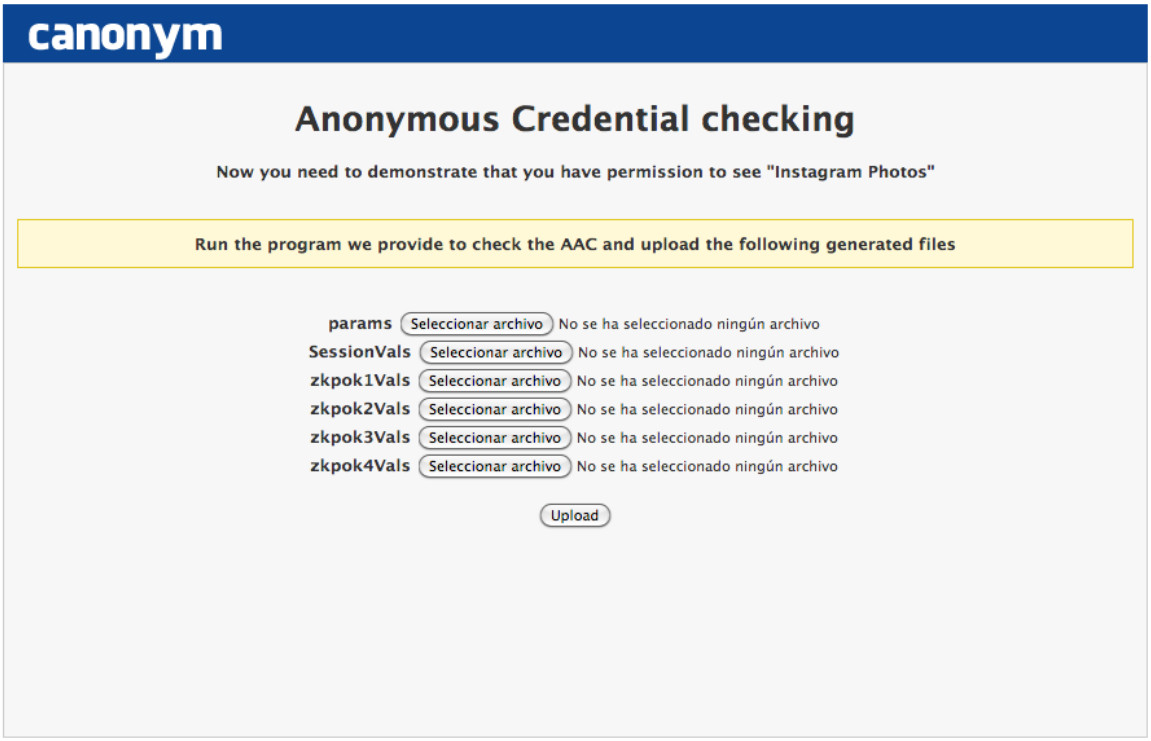

Figura 52. Introducir ficheros en CANONYM

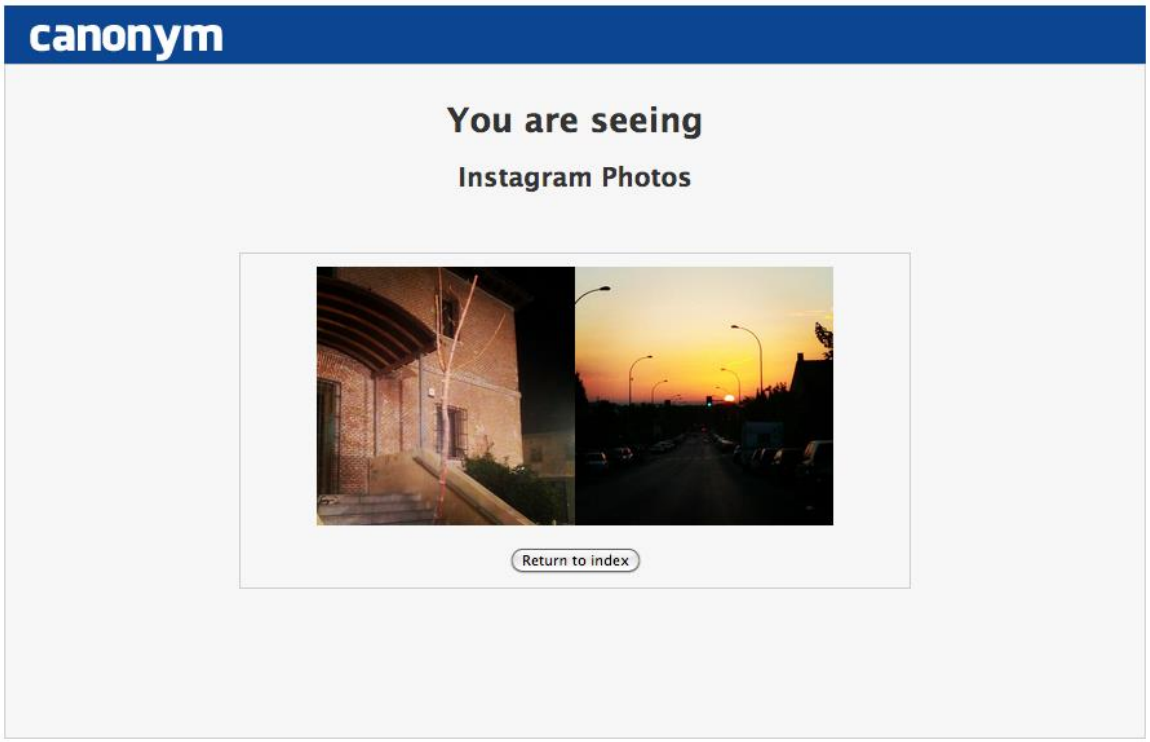

Figura 53. Visualización del álbum en CANONYM

Anexo 3

Plantillas

1. Plantilla definición textual de los casos de uso

Id: Identificador	
Nombre:	Nombre del caso de uso
Autor:	Autor del caso de uso
Descripción: Breve descripción de la función a cumplir por el caso de uso.	
Actores: Entidad que desarrolla la acción.	
Precondiciones: Condiciones previas para que pueda darse el caso de uso.	
Poscondiciones: Condiciones posteriores a que se haya producido el caso de uso.	
Flujo normal: Flujo de acciones que deben realizarse para que se realice el caso de uso.	
Flujo alternativo: Flujo alternativo de acciones derivadas del flujo normal.	

Tabla 23. Plantilla definición textual de los casos de uso

2. Plantilla especificación de requisitos

Requisitos de Software				
Tipo: Tipo de requisito				
Id	**Nombre**	**Descripción**	**Estabilidad**	**Prioridad**
Identificador	Nombre del requisito	Breve descripción del requisito.	Nivel de estabilidad. (Alto/Medio/Bajo)	Nivel de prioridad. (Alta/Media/Baja)
Tipo:				
Id	**Nombre**	**Descripción**	**Estabilidad**	**Prioridad**

Tabla 24. Plantilla especificación de requisitos

3. Plantilla pruebas de aceptación

Pruebas de aceptación			
Id	**Requisitos probados**	**Entrada**	**Salida**
Identificador	Identificador de los requisitos probados	Condiciones en las que debe realizarse la prueba.	Resultado esperado tras la realización de la prueba.

Tabla 25. Plantilla pruebas de aceptación